EQUITY FELLOWSHIP REPORT

Centring equity in data and digital governance:

Informing policy to empower practice

Bret Stephenson
La Trobe University
2024 ACSES Equity Fellow

2026

Universities For All

acses.edu.au

ACSES Australian Centre for Student Equity and Success

Curtin University

LA TROBE UNIVERSITY

Centring equity in data and digital governance: Informing policy to empower practice

25 June 2026

Dr Bret Stephenson, La Trobe University

Suggested citation: Stephenson, B. (2026). *Centring equity in data and digital governance: Informing policy to empower practice* (Equity Fellowship final report). Australian Centre for Student Equity and Success, Curtin University.

Australian Centre for Student Equity and Success
Tel: +61 8 9266 1573
Email: acses@curtin.edu.au
Web: www.acses.edu.au
Building 100
Curtin University
Kent St, Bentley WA 6102 | GPO Box U1987, Perth WA 6845

ISBN 978-1-7647025-0-8

Acknowledgement of Country

The Australian Centre for Student Equity and Success acknowledges Indigenous peoples across Australia as the Traditional Owners of the lands on which the nation's campuses are situated. With a history spanning more than 60,000 years as the original educators, Indigenous peoples hold a unique place in our nation. We recognise the importance of their knowledge and culture, and reflect the principles of participation, equity, and cultural respect in our work. We pay our respects to Elders past, present, and future, and consider it an honour to learn from our Indigenous colleagues, partners, and friends.

Acknowledgements

I would like to begin by sincerely thanking the many student equity practitioners and senior leaders who took part in the interviews for this research and generously shared their time, insights, and experiences. Your willingness to speak openly and reflect deeply on complex questions has been invaluable to this project. I recognise that this Fellowship report cannot fully capture the depth of your contributions; I hope future publications will address remaining gaps and extend the insights that could not be fully explored here.

This Fellowship would not have been possible without the support of the Australian Centre for Student Equity and Success (ACSES), which generously funded this work. I especially thank Professor Ian Li, ACSES Research and Policy Program Director, for his support and guidance throughout the Fellowship. I am also grateful to the entire ACSES team for their professionalism and generosity at every stage of the Fellowship. Working with you has been a pleasure.

This Fellowship project has benefited tremendously from the help, advice, and guidance of many experts in student equity research, practice, and policy. I especially thank Matt Brett (Deakin University), Darlene McLennan (ADCET), Andrew Harvey (Griffith University), Wojtek Tomaszewski (The University of Queensland), Gail Crimmins (University of the Sunshine Coast), Peter Bentley (Innovative Research Universities), and Tim Pitman (ACSES). The work of this Fellowship has also benefited greatly from the input, feedback, and guidance of my fellow Fellows across the year: Tracy Woodroffe (Charles Darwin University), Danielle Keenan (University of Technology Sydney), Darren Garvey (Curtin University), Peter Anderson (Griffith University), and Amani Bell (The University of Sydney). It has been a pleasure to share this process with you; thank you for your ongoing friendship and support.

Those acknowledged here represent only a fraction of the many people I have met and learned from during this Fellowship, and I emphasise that the findings, conclusions, and recommendations presented in this report are mine alone. A central idea running through this Fellowship is that equity work is data work—and that data about people are inherently political. Accordingly, any errors or omissions are my own.

Finally, thank you to my family for your love, support, and patience throughout this challenging year of Fellowship work.

Table of contents

Abbreviations

ACSES	Australian Centre for Student Equity and Success
ADM	automated decision-making
AI	artificial intelligence
AIATSIS	Australian Institute of Aboriginal and Torres Strait Islander Studies
ACU	Australian Catholic University
ANU	Australian National University
APPs	Australian Privacy Principles (*Privacy Act 1988*)
ATAR	Australian Tertiary Admission Rank
ATEC	Australian Tertiary Education Commission
DSP	Disability Support Program
FiF	first-in-family
GenAI	generative artificial intelligence
HESA	*Higher Education Support Act 2003* (Cth)
HREC	Human Research Ethics Committee
LAP	Learning Access Plans
LMS	learning management systems
NESB	non-English speaking background
OAIC	Office of the Australian Information Commissioner
PIA	privacy impact assessment
PRIS Act	*Privacy and Responsible Information Sharing Act 2024* (WA)
RQ	research question
SEHEEF	Student Equity in Higher Education Evaluation Framework
SES	socio-economic status
SfSP	Support for Students Policy
SRQ	sub-research question
TAC	Tertiary Admissions Centre
TCSI	Tertiary Collection of Student Information
TEQSA	Tertiary Education Quality and Standards Agency
UDL	Universal Design for Learning
UNDA	University of Notre Dame Australia
UOW	University of Wollongong

1. Executive summary

The Australian higher education sector is navigating a period of rapid digital transformation alongside major legislative reforms aimed at strengthening data privacy and enabling public sector data sharing. This shift coincides with sweeping national higher education policy reform, driven by the Australian Universities Accord's call for significantly expanded student equity data collection. This expansion is intended to underwrite new funding models, improve equity program evaluations, and ensure accountability.

The intersection of digital transformation and evolving higher education policy creates a strategic tension: while richer equity datasets are crucial for advancing policy goals, they contain sensitive personal information that heightens privacy, fairness, and governance risks. These risks are not hypothetical—misuse, overcollection, and poor transparency disproportionately affect equity cohorts. Yet the findings of this Fellowship suggest that many Australian universities remain significantly underprepared to meet the complex governance and ethical challenges these data require.

1.1 Research objective and questions

Against this backdrop of intersecting challenges, research on data governance in Australian universities, particularly regarding sensitive student equity data, remains critically limited. This ACSES Equity Fellowship addresses that gap by examining three central research questions (RQs):

> **(RQ1)**: What are the current and emerging legislative and regulatory frameworks for data privacy in Australia, and how might pending reforms affect universities and the governance of student equity data?
>
> **(RQ2)**: How do Australian universities approach data and digital governance in their policies, and to what extent do these frameworks consider or prioritise student equity?
>
> **(RQ3)**: What challenges and opportunities do student equity practitioners and senior university leaders identify in balancing the value and risks of student equity data within current governance frameworks and cultures?

1.2 Methodology

The research employed a multi-level, mixed-methods design, structured according to the "data work in context" framework (Foster et al., 2018), which examines data governance across macro, meso, and micro levels. The scope encompassed three interconnected streams of inquiry:

1. a review of the changing Australian legislative landscape relating to data privacy (macro level, RQ1)
2. a systematic content analysis of hundreds of university policies related to data governance, privacy, and student support (meso level, RQ2)

3. a qualitative study based on in-depth, semi-structured interviews with 21 university student equity practitioners and senior leaders (micro level, RQ3).

This integrated approach provides a grounded and holistic view of governance gaps, practitioner experiences, and opportunities for systemic reform.

1.3 Key findings

The findings reveal that Australian universities face significant and largely unresolved governance challenges in relation to student equity data, spanning three interconnected levels.

The privacy and regulatory landscape is fragmented and in transition. Australia's privacy framework remains a patchwork of Commonwealth, state, and territory legislation that creates significant ambiguity for universities navigating their governance obligations. Reforms underway, including proposed amendments to the *Privacy Act 1988* (Cth), signal a clear direction towards more proactive, rights-respecting models of data governance, including privacy-by-design. However, the pace and unevenness of reform mean universities are operating amid shifting and sometimes contradictory obligations, with limited sector-specific guidance to support consistent practice.

Institutional policy frameworks are fragmented, siloed, and poorly equipped to govern equity data. Systematic analysis of policies across 39 Australian universities found that privacy, data governance, learning analytics, artificial intelligence (AI), and student support instruments frequently sit in separate silos, use inconsistent terminology, and are weakly cross-referenced. Students, staff, and even internal decision-makers are often unable to determine how equity-related data are collected, combined, and used, or what safeguards apply. The governance of grey data, including behavioural, inferred, and algorithmically derived information, falls largely outside existing frameworks.

Frontline equity staff and the students they serve bear the consequences of governance failure. The qualitative study, drawing on interviews with 21 equity practitioners and senior leaders, reveals the practical and ethical toll of these structural gaps. Staff routinely navigate ethically complex data decisions without adequate guidance, escalation pathways, or institutional protection. Growing demands for data-intensive evaluation, accelerated by the Australian Universities Accord, are intensifying pressure on universities to collect and use sensitive equity data faster than governance structures can support. Significant ethical burdens are shifted onto individual staff members rather than systems, while the student communities most affected bear disproportionate risk.

1.4 Recommended actions

Ethical and equity-centred data governance is not merely a compliance obligation—it is a condition for advancing student equity in the digital age. The report's nine recommendations are directed at four audiences.

The Australian Government Department of Education should embed privacy and data governance safeguards across the equity policy life cycle and explicitly permit equity

program funds to support governance capability uplift in universities. The Australian Tertiary Education Commission (ATEC) and the Tertiary Education Quality and Standards Agency (TEQSA) should collaborate to establish a national baseline for student equity data governance and develop shared, sector-specific tools to drive consistency across a fragmented landscape.

For universities, the recommendations are both the most numerous and the most operationally immediate. They should adopt standards above legal minima and implement privacy-by-design; harmonise their data, digital, and equity policy frameworks; establish defined oversight pathways for evaluation activities outside Human Research Ethics Committee (HREC) review; embed participatory governance with paid student and staff co-design; and ensure frontline equity support is backed by resourcing, clear policy, and safe escalation.

Finally, peak bodies and professional associations should co-design and publish field- and cohort-specific practice standards and exemplars for ethical equity data governance.

What is at stake is trust, and the communities most affected by these practices must have a genuine voice in shaping them.

2. Recommendations

2.1 Recommendations for government and policymakers

Recommendation 1: The Australian Government Department of Education should embed privacy, data, and digital governance safeguards across the equity policy life cycle—design, implementation, and evaluation.

Recommendation 2: The Australian Government Department of Education should permit equity program funds to support privacy-by-design, ethical evaluation, and equity data governance capability in universities.

2.2 Recommendations for sector steward and regulator: ATEC and TEQSA

Recommendation 3: ATEC and TEQSA should collaborate to establish a national baseline for student equity data governance and provide shared, sector-specific tools to drive consistency across a fragmented landscape.

2.3 Recommendations for universities

Recommendation 4: Universities should adopt standards above legal minima and implement privacy-by-design and robust data and digital governance.

Recommendation 5: Universities should harmonise digital and data policy frameworks and centre equity across the policy suite.

Recommendation 6: Universities should establish defined oversight responsibilities for equity-related evaluation activities that fall outside HREC review.

Recommendation 7: Universities should embed democratic and participatory data governance and resource co-design with students and staff.

2.4 Recommendations for senior university leaders, peak bodies, and professional associations

Recommendation 8: Senior university leaders should ensure frontline equity support operates under a robust privacy-by-design data culture—backed by resourcing, clear policy, and safe escalation.

Recommendation 9: Peak bodies and professional associations should co-design and publish field- and cohort-specific practice standards and exemplars for ethical equity data governance.

3. Introduction and background

Rapid digital transformation is reshaping how governments and universities collect, manage, and utilise student data. In Australia, this shift is occurring alongside significant legislative reform aimed at strengthening data privacy (Attorney-General's Department, 2022), enabling greater public sector data sharing (*Data Availability and Transparency Act 2022* [Cth]), and guiding the responsible adoption of emerging technologies such as AI (Department of Industry, Science and Resources, 2024).

At the same time, national higher education policy is also undergoing sweeping reforms. The Australian Universities Accord (the Accord) has urged the Australian Government to adopt more ambitious equity targets and significantly expand student equity data collections (Department of Education, 2024a). These data are needed to underwrite new equity-focused "needs-based" funding arrangements (pp. 288–296), to better inform policy decisions, and "to measure progress, evaluate what works at a system level, and ensure accountability" (p. 111).

These two developments—digital transformation and sweeping changes to higher education equity policy—are converging within university data and digital governance systems, creating both new opportunities and complex risks. These challenges are especially pronounced for student equity cohorts.

As this ACSES Equity Fellowship research demonstrates, equity practitioners and university leaders are eager to harness data and digital technologies that support student autonomy, wellbeing, and success. Yet their work remains grounded in strong personal and professional commitments to student privacy, ethical data use, and the imperative to build and sustain trust.

This is especially critical given that even in their most basic, binary forms, student equity data necessarily contain personal, private, and often highly sensitive cultural, financial, and health information regarding both individuals and groups. In this light, equity data are risky data and particularly vulnerable to potential misuse and the production of "data harms" (Pangrazio, 2024).

At the same time, there is a widespread and persistent need for better and more meaningful equity data across the sector. Equity practitioners, researchers, and university leaders alike consistently report deep frustration with the quality, accessibility, and relevance of existing data systems. It is for this reason that the Accord's final report calls on the Australian Government to pursue a program of what it terms "enhanced" equity data collection: "In addition to setting [equity] targets, Government must improve data collection to understand and address more granular indicators of disadvantage better" (Department of Education, 2024a, p. 117).

Alongside "more granular" data, the Accord also seeks more sensitive data, recommending an expanded equity data and reporting framework to monitor previously unrecognised equity groups, including first-in-family (FiF) students, mature-age students, care leavers, refugees, carers, certain language groups, and prisoners (Department of Education, 2024a, p. 117).

Although such data are essential to advancing student equity, their collection, management, and use involve a complex interplay of risks, responsibilities, and competing interests. Without robust governance and risk management systems, universities may inadvertently undermine their equity goals, entrench existing inequalities, and shift institutional risks onto students themselves, or the already overburdened staff responsible for providing high-quality support.

Achieving these goals, in line with the Accord's objectives, demands a strong, consistent, and sector-wide commitment to transparency, accountability, and meaningful stakeholder involvement in data and digital governance. The challenge is not merely technical; it also requires embedding responsible, accountable, and equity-centred governance within institutional data cultures.

3.1 Project rationale

In a context of increasing regulatory complexity and heightened expectations for institutional accountability via enhanced data collection, analysis, and sharing, research on the unique challenges faced by Australian universities in governing student data remains notably scarce.

A recent study by McNicol et al. (2024) provides a notable exception, exploring the unique challenges of enterprise data governance programs in Australian universities, though it does not focus specifically on student equity data. This research gap is even more acute given the sensitivity and increased risks involved with student equity data.

While very little is known about data governance practices in Australian universities, even less is known about how equity data practices are understood, contested, and enacted by those directly engaged in what is collectively referred to as "equity work" in this report. The perspectives of equity practitioners, researchers, and university leaders—those tasked with navigating the tensions between institutional demands, professional ethics, and student trust—remain largely absent from the literature. As the sector moves towards a more expansive and granular data regime, amid ongoing legislative privacy reforms, there is an urgent need to understand these emerging challenges as experienced by those doing this critical work within Australia's universities.

3.2 Concepts

3.2.1 Equity work as data work

As a step towards filling this gap, this project foregrounds student equity work as data work—a concept used here to highlight the often underappreciated, yet essential tasks involved in producing, managing, interpreting, and communicating data within various organisational settings (Foster et al., 2018; Møller et al., 2020). Data work, as a concept, extends beyond purely technical function; it encompasses the broader sociotechnical elements referred to in this report as data and digital governance:

> Data work is also concerned with the human and ethics. It interfaces with people's questions, rights, and concerns about data and includes the tasks of managing and mitigating those concerns. (Møller et al., 2020, p. 52)

While the concept of "data work" can be applied to many organisational settings, it has gained particular currency in health care (Jarke & Büchner, 2024; Møller et al., 2020), where the parallels with student equity work, particularly that of disability support and advising, are apparent. Equity practitioners similarly engage in regular data-related tasks—often alongside, but in some cases, fully integrated within their primary roles—to identify students in need of support and to help ensure their success.

By foregrounding equity work as data work, this report emphasises the central role of student equity practitioners in organisational and sector-wide aspirations to become increasingly data driven, evidence based, and data informed. While equity work has always carried elements of data work, organisational "data care arrangements" (Jarke & Büchner, 2024)—or the responsibility for data production, maintenance, and responsible use—are increasingly delegated to practitioners of all types, including those who are not formally trained data professionals. In other words, "data care" is now a core duty for nearly all student equity practitioner roles within Australian universities.

Moreover, with the sector now embracing the need for widespread and rigorous evaluation of student equity programs, in the pattern established by the *Student Equity in Higher Education Evaluation Framework* (SEHEEF) (Robinson et al., 2021), equity work is becoming further intertwined with data work. Such work requires careful attention, negotiation, and management to ensure the responsible handling of sensitive student data (Jarke & Büchner, 2024).

3.2.2 Data and digital governance

This report adopted an integrated approach to data and digital governance, recognising that in contemporary university contexts, these domains are deeply interconnected. Consequently, a singular focus on data alone is insufficient to capture the broader sociotechnical systems that now shape universities. The full spectrum of digital technologies used to produce, collect, and utilise student data must also be considered. In brief, of concern is not just the personal data of students but also the digital technologies they empower and the purposes they are put to.

Emerging scholarship on "postdigital education" (Fawns, 2023; Hayes et al., 2024) and "sociodigital futures" (Sriprakash et al., 2024) emphasises that digital technologies are not simply layered onto existing educational systems. Rather, they are embedded in the daily practices that shape how educational relationships, decisions, and values are formed.

In this view, both data and digital technology systems influence who is involved in decision-making and how educational purposes are defined. Therefore, this report treats data and digital governance as overlapping, mutually reinforcing areas of institutional practice and concern.

Researchers have identified two forces that are central in this context. The first is "datafication", or the ever-increasing transformation of social processes into quantifiable data (Mejias & Couldry, 2019). The second is "digitalisation", referring to the widespread embedding of digital systems and technologies across university operations (Komljenovic,

2022). Together, they raise complex questions about institutional responsibility, oversight, and ethics in the handling of student data, and thus must be considered in tandem.

A second challenge for data and digital technology governance in Australian universities is twofold: determining which technologies require oversight and defining what form that governance should take.

This report uses the term “digital” in a deliberately broad sense, covering the full range of existing and emerging technologies embedded across the higher education sector. The original proposal for this Fellowship used the term “data and AI governance”, but over the course of 2024 it became clear that institutional conversations were dominated by a single technology: generative AI (GenAI). These discussions often focused narrowly on concerns related to assessment integrity and the potential for academic misconduct.

For example, in June 2024, TEQSA asked all registered higher education providers to assess the impact of GenAI on research, teaching, learning, and assessment, and to submit institutional action plans detailing how each institution would work to uphold academic standards (TEQSA, 2024, p. 2). While it is an appropriate measure, this focus on GenAI has left little room for a sector-wide consideration of other digital technologies—many of which are data intensive and already deeply embedded—that carry equally significant risks to student equity and overall educational quality.

Well before the rise of GenAI, the widespread adoption of predictive and prescriptive analytics in universities had already raised concerns regarding algorithmic bias and its potential to reinforce existing inequalities (Baker & Hawn, 2022; Stephenson et al., 2022). Others have raised concerns regarding the commercial dominance of for-profit digital platforms in universities (Komljenovic, 2021) and the subsequent erosion of student privacy these platforms can cause (Sheridan, 2022).

This Fellowship project has identified a wide range of institutional policies referring to digital technologies beyond GenAI, including learning analytics, predictive modelling, assistive technologies, and broader AI systems. These technologies raise complex governance and equity issues and deserve the same scrutiny that is currently applied to GenAI. Moreover, the inconsistent terminology used across institutional policies—sometimes even within a single institution—complicates governance and weakens transparency.

For these reasons, this report uses the broader term “digital” to describe technologies that generate, capture, and utilise student data. It also calls for clearer and more consistent language, and for harmonised governance approaches across institutions and policy domains.

3.2.3 What is governance?

This Fellowship report defines data and digital governance as the collection of formal structures, policies, roles, and decision-making processes that guide how data and digital technologies are responsibly used and managed in universities. These include institutional mechanisms—such as oversight committees, role-based responsibilities, and internal policies—as well as broader macro-level frameworks, such as legislation, regulatory standards, and national sector guidelines. Collectively, these layers of governance not only determine how student data are collected, secured, interpreted, and shared but also shape who is included or excluded in key decisions.

For this reason, the report also advocates for governance models that are meaningfully participatory and democratic, engaging students, staff, and other community stakeholders in decision-making processes (Knight et al., 2023; Sloane et al., 2022; Stephenson & Harvey, 2022). The work of Cheong and Nyaupane (2022) on “smart campuses” has underscored this need, showing that weak or opaque governance structures can erode trust, foster confusion, and leave students feeling surveilled or coerced.

Raaper and Komljenovic (2022) argued a similar point, observing that universities were being increasingly subsumed by the digital economy. They argued that students are increasingly positioned as passive “data subjects” rather than active participants in institutional governance (p. 23). While formal student representation may exist, the digital data that students are compelled to generate, through their interactions with digital university platforms, are often used to inform decisions without their knowledge, consent, or involvement.

In response, these scholars and others have advocated for a renewed focus on participatory governance models, warning that a lack of such oversight risks disempowering students and undermining institutional accountability (Dollinger & Lodge, 2019; Stephenson & Harvey, 2022; Swist et al., 2024).

3.3 Research aims

While equity work has long been deeply embedded in data work, the current era of rapid digital transformation and significant legislative change makes it critically important to better understand this relationship and the challenges and opportunities it presents. Section 7 of this report shows that many equity practitioners and senior university leaders have a sense that institutional data-handling and governance practices are not fully mature or lack clarity. Many of the research participants expressed sentiments similar to one particularly pithy remark shared early in the project: “We do an awful lot of work in the grey, don’t we?”

This report contextualises participants’ uncertainty, details the complexities of handling sensitive student data in equity practice, and provides practical recommendations for government, universities, and practitioners working in the grey zones where equity and data governance meet.

To guide this inquiry, the research was structured around three core research questions (RQs):

> **(RQ1):** What are the current and emerging legislative and regulatory frameworks for data privacy in Australia, and how might pending reforms affect universities and the governance of student equity data?
>
> **(RQ2):** How do Australian universities approach data and digital governance in their policies, and to what extent do these frameworks consider or prioritise student equity?
>
> **(RQ3)**: What challenges and opportunities do student equity practitioners and senior university leaders identify in balancing the value and risks of student equity data within current governance frameworks and cultures?

Together, these primary RQs shape the structure and focus of the report, but they are supplemented by sub-research questions (SRQs) where needed to provide additional clarity and granularity. For example, an important SRQ is explored in Section 4: “What counts as student equity data, and why centre equity in data and digital governance?”

3.4 Report structure

This Fellowship sought to illuminate the complex tensions, challenges, and opportunities that arise as student equity work increasingly intersects with data and digital practices in Australian universities. To guide this inquiry, the Fellowship and its final report were structured around the “data work in context” framework proposed by Foster et al. (2018).

According to Foster et al. (2018), data work involves creating value through organising, analysing, interpreting, and using data to inform decisions. However, they also emphasised that such work entails significant risks—including ethical issues related to ownership, privacy, and trust, as well as practical concerns such as data breaches and algorithmic bias. Effective governance is necessary to manage these risks and must operate across three interconnected levels:

1. macro-level national laws and sector-specific regulations
2. meso-level organisational policies, cultures, and governance mechanisms
3. micro-level conditions experienced by professionals involved in data work.

This framework highlights that micro-level data work—how individuals balance the value of data against their inherent risks—does not happen in a vacuum. Rather, it is shaped by the cascading effects of legal, regulatory, and institutional systems. Equity practitioners operate within these overlapping and occasionally contradictory layers of national and state legislation, sectoral norms, and institutional cultures. These structures can either enable or impede efforts to make equity data both useful and safe.

Section 4 of this report asks, “What counts as student equity data, and why centre equity in data and digital governance?” The section critically re-examines what counts as “equity data” in Australian higher education. It traces the origins and limitations of the official equity data framework and highlights the growing relevance of incidental, behavioural, and algorithmically inferred data in increasingly digital university systems. The analysis advocates for a more expansive and risk-based approach to equity data governance—one that addresses emerging risks, collective harms, and the relational nature of data in a digital era.

Section 5 shifts the focus to the question, “What are universities required to do?” Addressing RQ1, it places this expanded view of equity data within the broader context of macro-level governance. The section outlines Australia’s fragmented privacy law framework, reviewing key national, state, and territory legislation, policies, and regulatory structures that affect the university sector. It also explores how current debates and proposed reforms in privacy and digital governance should inform a stronger, more coherent vision for data governance in support of equity goals.

Section 6 asks, “What do universities say they will do?” Addressing RQ2, it presents a summary analysis of hundreds of publicly available policies across Australian universities, examining how institutions are currently approaching data and digital governance. It pays

particular attention to how student equity considerations are addressed, prioritised, and sometimes overlooked within these frameworks.

Section 7 turns to practice, asking, “What is the experience of equity practitioners working within these governance structures?” Addressing RQ3, this section presents the Fellowship’s most substantive contribution: high-level findings from a qualitative study involving 21 equity practitioners and senior university leaders from across the sector. Participants described a complex operational landscape in which they are expected to collect, interpret, and act on equity-related data—often involving sensitive personal information—while also upholding their professional and ethical obligations to student privacy and wellbeing.

Their accounts reveal persistent tensions between recognising the value of student data and managing its significant risks. Institutional policies and governance systems were often seen as vague, fragmented, or disconnected from the realities of equity work. Many participants spoke of working “in the grey”, where they must bridge policy gaps, translate abstract principles into practice, and make ethical decisions in the absence of clear guidance. By bringing these everyday experiences to the forefront, the report provides a grounded view of the many challenges that equity practitioners must navigate in an increasingly data-driven environment.

Finally, Section 8 summarises the report’s recommendations.

Reader’s note. Some sections of this report include a brief “bridge note” linking the discussion to specific recommendations. Bridge notes are used sparingly and appear in italics with recommendation numbers in bold, for example: *This section supports **R5** (harmonise frameworks) and **R3** (national baseline and shared tools).*

4. What counts as student equity data?

Australian higher education student equity policy has long been a markedly data-dependent and numbers-driven enterprise (Gale, 2012), and in this light, "equity work" has always been "data work". Consistent with this data dependency, "equity" itself has been largely understood in statistical terms: its goal is achieved primarily by seeking the "proportional representation" of identified groups (Harvey et al., 2016). This section serves two purposes: to re-examine what constitutes "equity data" in Australian higher education and to detail the substantial data governance challenges that a more refined view brings to the forefront.

*This section frames the case for **R3** (national baseline and shared taxonomy), **R4** (privacy-by-design in practice), and **R5** (harmonised policy suite).*

4.1 The legacy equity data framework

Nationally uniform methods for quantifying student equity were first systematised following the publication of *A Fair Chance for All* (Department of Employment, Education and Training, 1990), the Australian Government's landmark higher education equity policy paper. Among its many contributions, the paper identified six core underrepresented groups that would remain the focus of student equity policy over the ensuing decades.

While *A Fair Chance for All* set the broad policy strokes for student equity, the Martin Committee later took responsibility for establishing standardised definitions for the six core "equity groups"[1] and introducing a standard suite of equity performance metrics—commonly known as the "Martin Indicators"—that could be adopted and applied across the sector (Martin, 1994).

This original national "equity framework" has remained remarkably consistent over subsequent decades. Minor adjustments have been made to group definitions, including calculation methods and naming conventions, while governments have periodically changed policy aims, targets, and the funding allocated to each group. Current Australian higher education policy prioritises four key equity groups, now often referred to as "target" or "priority" groups:

- students from low socio-economic status (SES) backgrounds
- First Nations Australian students (or Aboriginal and Torres Strait Islander students)
- students from regional or remote areas
- students with disability.

[1] In the interest of clarity, consistency, and alignment with Australian higher education policy conventions, this report uses the terms "equity groups", "equity students", and "equity" in a general sense. However, the fact that these terms are contested and often replaced by alternatives such as "target groups", "priority groups", or "equity-deserving groups" is acknowledged.

Of the original six equity groups, two are no longer a core focus of government policy, a shift highlighted in a review by Tomaszewski et al. (2018) and recently reflected in the Accord final report (Department of Education, 2024a). These groups are:

- women in non-traditional areas
- students from non-English speaking backgrounds (NESBs).

The creation of the original six core groups was not without controversy. As Martin (2016) later reflected, universities were initially reluctant to share detailed student data with the government, citing concerns about institutional autonomy, administrative burden, and the sensitivity of certain types of data—particularly data relating to students with disability (see also Brett, 2016).

As a result, the equity group measures were designed to prioritise simplicity, or data minimisation, and were based almost exclusively on the use of existing university administrative data. For this reason, the resulting legacy equity framework is suited primarily for high-level monitoring of just six core equity group participation and outcome rates rather than for determining individual levels of educational disadvantage (Martin, 2016, p. 31).

4.2 Towards a more refined equity data framework

The data used to identify the four “target” or “priority” cohorts described above are what are commonly thought of as “equity data” or, perhaps, “official equity data”. Australian universities are required by government to collect and report these specific forms of student equity data to the Department of Education via the Tertiary Collection of Student Information (TCSI). In this way, these official student equity data are used by government and universities to fulfil statutory responsibilities.

This external reporting serves to fulfil accountability and transparency obligations under the *Higher Education Support Act 2003* (Cth) (HESA), thereby enabling government to allocate funding, monitor equity group representation and outcomes, and inform evidence-based national policy and reporting. Universities will also use these “official” equity data collections for their own internal purposes. Because of their relatively low dimensionality and fidelity, these data are sometimes described as “binary” or “dichotomous” categories (Tomaszewski et al., 2018), reflecting their largely unrefined “yes” or “no” nature. This is made particularly clear in the way they are often presented in statistical analyses (for example, low SES versus not low SES).

The blunt and unrefined nature of the “official” or legacy framework and data collections has led to a large body of research indicating the need for more numerous, and more granular, indicators of disadvantage. These calls for enhanced data collections have focused largely on three broad approaches to the expansion or improvement of equity data collections. Each creates its own mix of value and risk generation that must be addressed through effective governance.

First, many proposals have argued for the formal recognition of additional “equity groups” within the national equity framework. This includes calls for enhanced data collection and reporting on students from a variety of backgrounds, personal circumstances, population

groups, and other characteristics, including histories of personal hardship (Tomaszewski et al., 2018).

As mentioned earlier, the Accord has called for official data collections and reporting to be expanded to include FiF students, mature-aged learners, care leavers, refugees, carers, certain language groups, and prisoners (Department of Education, 2024a, p. 117). The wording used in the Accord's final report suggests that some of these groups should be considered for full "target cohort" or "equity group" membership at a future time—as determined by ATEC—while indicating that other groups may require enhanced data for monitoring purposes only.

Second, other proposals have stressed the need for more refined and granular data to be captured for the existing core equity groups. For example, acknowledging the many pitfalls of area-based indicators of SES, researchers have suggested individual-level measures—including more refined data on parental education and occupation, or other direct measures of family income (see Tomaszewski et al., 2018, for a full discussion). While such proposals are likely to increase the value of SES indicators, they are also certain to increase the risks relating to privacy and data governance.

Third, proposals have also centred on the perceived need for greater recognition of intersectionality—or the cumulative disadvantages associated with multiple equity group membership. In their extensive review of cumulative disadvantage, Tomaszewski et al. (2020) tested five prototype measures (A–E) using data collected for the four primary "equity groups" (low SES, First Nations, regional or remote, and disability). The authors found these existing data sufficient for developing the new measures.

However, although no additional data sources may be required as inputs, the prototype measures would generate new forms of equity data if adopted within the framework, including individual scores, composite scores, and categorical indices of disadvantage. As discussed below (Section 4.4.4), these new and expanded data forms raise further challenges for privacy and data governance. Tomaszewski et al. (2020) were clearly alert to this risk, advocating for the development of ethical data governance guidelines before any implementation.

For its part, the Accord final report (Department of Education, 2024a) has recommended that the loadings for its proposed "needs-based funding" system "should recognise the cumulative and compounding effects of disadvantage" (p. 138). While it stops short of proposing a specific measure for cumulative disadvantage, or its wider adoption, it suggests that these decisions should be made by ATEC upon its establishment.

4.3 Derived and disclosed equity data

Understanding equity data requires distinguishing the two principal types of data that support core equity group identification: derived data and self-disclosed data. When viewed through a data governance lens, each presents a critical trade-off between value and risk.

First, derived data involve the creation of new information by processing, analysing, or combining existing raw data according to human-defined rules or formulas. For example, the definitions for low SES and regional students are derived by linking a student's postcode(s)—used as a geographic indicator—with Australian Bureau of Statistics Census

data. As relatively coarse, area-based proxies, both definitions have been widely critiqued for their limited precision and questionable utility in accurately identifying individual disadvantage (Tomaszewski et al., 2018).

Less frequently acknowledged, however, is that students are automatically assigned to these derived equity categories without explicit notification or consent. From both data governance and equity practitioner perspectives, this lack of transparency can raise significant concerns. These concerns are particularly acute for the low SES category because most students are likely unaware that they have been classified, and potentially targeted for support, according to a proxy indicator for SES. The combination of limited accuracy and low transparency restricts the utility of these data, a view strongly echoed by participants in this research.

In addition to the four priority equity groups, such as low SES and regional or remote students, several other less-recognised categories—what Crawford (2022) described as "equity-like" groups—can also be identified through the combination of existing TCSI data elements that are collected for government reporting.

For example, legacy equity groups such as women in non-traditional areas may be derived through the combination of gender (E315) and field of education (E461) TCSI data elements. Similarly, and although now seldom used, students from a NESB could be derived through three different data elements: citizen resident code (E358), year of arrival in Australia (E347), and language spoken at home (E348).

FiF status, according to some proposed definitions, may be identified from student reports of their parents' level of educational attainment (E573 and E574) (O'Shea et al., 2024). Furthermore, while no specific field for refugee status exists, very limited information can be derived from the student's reported visa status using the TCSI data element E358 (citizen resident code), specifically the value for a permanent humanitarian visa (Molla, 2021). Lastly, mature-aged students—also referred to as mature and returning students (MARS)—may be identified directly from the date of birth information institutions already submit; however, deriving this status is complicated by the fact that universities do not use a standardised age threshold.

The second broad data type consists of self-disclosed or self-identified equity groups, specifically First Nations Australian students and students with disability. These data are typically collected directly from the student during the enrolment process, but disclosures can also be made or withdrawn at any point during their studies. Importantly, and unlike most of the derived equity categories, self-disclosed equity group membership may be represented in datasets as either static or dynamic characteristics because a person's status can change over time.

The reliance on self-disclosure for these groups has raised concerns about both under- and over-reporting, partly because of variations in collection and reporting methods across institutions (Tomaszewski et al., 2018). A rich body of research now details the barriers and hesitancy many students experience when asked to disclose these identities or statuses to their universities or to government (Clark et al., 2019; Grimes et al., 2017; Hollinsworth et al., 2021). For example, Grimes et al.'s (2019) study of students with disability found that some participants withheld or revoked disclosures because of concerns about privacy, lack of control over internal university disclosures, and fears of stigma and discrimination.

Unlike derived equity data categories, self-disclosures of equity status are typically accompanied by data privacy collection notices. These notices should explicitly inform students about how, by whom, and for what purposes their personal information will be used.

While collection notices provide an important level of transparency, they still suffer from the many issues that have been identified with “notice and consent” models of privacy protection more generally (Manwaring et al., 2021). For example, there are persistent concerns regarding the clarity, consistency, and comprehensiveness of these notices. In practice, the complexity of privacy notices—or alternatively, their lack of specificity—can lead to familiar attitudes of privacy “resignation” or “cynicism” (Draper et al., 2024; Hoffmann et al., 2024).

Although a detailed discussion of the limitations of “notice and consent” data privacy regimes follows (Section 5.2.2), it is crucial to note a preliminary challenge: many university staff, including the participants in this research, often lack a clear understanding of how sensitive equity data are collected by their institutions, including the specific content of student privacy notices. In sum, while self-disclosed equity data are typically collected under conditions of stronger notice and consent, these measures do not represent a panacea for mitigating data harms.

4.4 The creation and collection of equity data

To continue refining our understanding of equity data, its multiple points of creation and collection are now considered, alongside the unique data governance challenges each mode creates. The focus here is on outlining four broad modes of equity data capture—systematic, incidental, indirect, and inferred—and briefly examining the value and risks presented by each. While the taxonomy is neither exhaustive nor without a measure of overlap, it provides a useful means for highlighting the true diversity of data production and its attendant governance demands.

4.4.1 Systematic data creation and collection

The most familiar mode of data capture is systematic collection, exemplified by the national TCSI collection. This approach represents the mandatory, sector-wide process that generates the “official” equity data used by government to inform policy formation and monitor sector performance. From a data governance perspective, the implementation of this systematic collection process yields several key benefits.

First, data elements within systematic collection are ideally sourced directly from the students themselves. Excluding instances when data are derived or merged with external indices (such as with low SES categorisation), this direct collection provides students with a foundational level of awareness and transparency regarding the personal information collected via TCSI.

Second, TCSI data collections operate under a clear legal foundation because the submission of these data elements is required by HESA. Furthermore, data collected under HESA and via TCSI are automatically subject to the federal *Privacy Act 1988* (Cth). This legal linkage provides essential sector-wide consistency regarding transparency, minimum requirements for privacy collection notices, and the broader data protections required by the Act (discussed more fully in Section 5).

Third, systematic collection underpins national standardisation and consistency, both essential for effective policy analysis. By mandating common data elements and definitions across institutions and over time, TCSI ensures the data remains reliable for longitudinal analysis and sector-wide comparability.

The benefits of systematic data collection are manifold, particularly its power to bring underrepresented or disadvantaged student cohorts to light. Consequently, equity stakeholders often advocate for expanding these collections to capture more groups and achieve greater data refinement, operating on the principle that what goes unmeasured also goes unaddressed and unfunded.

Despite the significant benefits of standardisation, systematic data capture systems such as TCSI face at least three major challenges. First, data capture is often undermined by significant under-reporting and missing data, a problem particularly acute for voluntary fields, where a lack of trust in institutional and government data collections may deter student disclosure. Second, the inherent inflexibility of a standardised system can lock in particular ways of representing groups and limit the utility of the data. The long-running debate over how to define and categorise students with disability illustrates this problem: established system categories are often criticised as being “not fit for purpose” (Pitman et al., 2023). Third, despite the national mandate, data collection practices can still differ significantly between institutions, creating disparities in data quality and reducing the veracity of national datasets. These inconsistencies have been especially evident in relation to the collection of disability data, as recognised by the Accord (Department of Education, 2024a, p. 116).

4.4.2 Incidental data creation and collection

In contrast to systematic collection, incidental equity data arises in two ways: (i) through the incidental creation of information as a by-product of routine interactions with the university (for example, advising notes, case management records, learning management systems [LMS] activity); or (ii) through non-systematic, local collection for administrative or support purposes. These data can surface equity-relevant needs, but they are not collected under a governance regime characterised by notice, consent, and transparency and therefore do not allow for the same range of uses as those seen with systematic data collections.

For example, care leaver status—students who have experienced out-of-home care—is seldom systematically captured by Australian universities. A study by McNamara et al. (2019) found that only one out of 28 universities systematically collected this status via optional disclosure (with the implied provision of a privacy notice). A further three universities indicated that disclosures were held in the confidential client records of student support services, demonstrating the highly incidental and privileged nature of these non-systematic records.

Military veterans have also been suggested for inclusion in national and institutional equity group data collections. A study by Harvey et al. (2018) found that approximately one third of veterans had “disclosed” this status to their university. These were, however, incidental disclosures, which included “supplying standard employment history, seeking credit for prior learning, and seeking access to support services” (p. 23).

In the absence of systematic and well-governed data collection practices, such incidental disclosures have limited utility. Nonetheless, they remain important forms of equity data that

present unique governance concerns, particularly when determining the scope of a reasonable secondary use. Moreover, these examples clearly illustrate that the data work supporting equity initiatives often extends well beyond official TCSI collections and the core target equity groups commonly recognised in government policy.

4.4.3 Indirect data creation and collection

The third mode of data capture is indirect collection, which may include captures of highly sensitive equity-related information disclosed by students to a third-party intermediary, rather than directly to the university or the government. This category includes, for example, the comprehensive data collected by State Tertiary Admissions Centres (TACs) for equity-focused special entry schemes and scholarships.

The TACs are generally independent, non-profit companies owned by their member universities. Accordingly, the sharing of this highly sensitive equity data is governed by contractual agreements between the TAC and the institution, rather than by the direct statutory mandates that govern systematic data collection. These bilateral contracts are the primary mechanism for governing such data. However, this approach creates opacity, as the agreements are typically inaccessible to data subjects. As a result, individuals may have limited capacity to understand or influence the use, protection, and disposal of their personal information (Krebs & Bennett, 2024).These schemes ask students to provide highly sensitive, and equity-relevant, information in exchange for benefits such as supplementary points credited to their Australian Tertiary Admission Rank (ATAR) or confirmation of eligibility for equity-focused scholarships. The disclosures required can be detailed and deeply personal, often including documentation such as medical reports to confirm disability status or detailed statements of financial or personal hardship. This makes special entry access schemes data among the most sensitive equity data collected within the sector, a point strongly reflected by many of the participants in this research.

Despite being highly detailed and capable of confirming individual disadvantage, the place of these indirect data in the broader equity ecosystem remains ambiguous, and their utility is limited. This paradox is primarily driven by the fact that the information is collected by an external body largely for a single purpose. Consequently, these third-party data are typically not systematically integrated into a university's general enterprise data, nor are they used for a range of possible secondary applications. They remain a key and often overlooked part of the equity data ecosystem in Australian higher education.

4.4.4 Inferred data creation and collection

The abovementioned modes of data creation and collection have focused largely on adjudicating a student's equity group membership or status. This report seeks to extend that view, contending that in the age of digitalisation and datafication, equity data must be understood as encompassing far more than traditional group classifications. The picture is complicated by a fourth, and increasingly critical, form of equity data creation: inferred data.

While inferred data are often treated as synonyms or subtypes of derived data (recalling the discussion of low SES and regional groups in Section 4.3), data scientists and law scholars frequently draw out essential differences between the two types, and for good reason. The

distinction hinges largely on the process of data creation, and the types of data used to create new, and previously unknown, data:

- Derived data rely on a low analytical leap, representing a direct, administrative calculation or classification (for example, classifying a student as mature-aged according to a provided birthdate).
- Inferred data, conversely, involve a high analytical leap based on probability, pattern recognition, or machine learning, creating wholly novel insights or predictions. (Custers & Vrabec, 2024, p. 5)

Despite this complexity, inferred data are frequently associated with “big data” and the use of powerful machine learning or predictive analytics techniques. For example, social media platforms may infer personal characteristics about users, even sensitive attributes, not based on data the user knowingly volunteers but through algorithmic inferences based on other behavioural data.

While inferred data are becoming increasingly widespread, two examples of inferred data that are presently part of the equity data ecosystem can be briefly highlighted: cumulative disadvantage scoring and predictive “at-risk” monitoring.

Once again, many of the approaches to calculating a composite cumulative disadvantage scoring (Tomaszewski et al., 2020), as mentioned in Section 4.2, are examples of inferred data. These scores are not collected from the student as a raw input but are instead mathematically, statistically, or algorithmically constructed inferences or predictions of disadvantage. Similarly, outputs generated by many forms of academic risk profiling and predictive analytics—sometimes described as learning analytics, propensity modelling, or risk scoring—would qualify as inferred data. In higher education, these processes are often used to infer a student’s likely risk of attrition, academic difficulty, progression, or success (Stephenson et al., 2022).

Inferred data carry many important implications for equity-deserving individuals and cohorts. Here the focus is on just three of these that carry important implications for the governance of student equity data.

First, it is important to recognise that inferences can identify, with a level of probability, what are considered equity group traits in individuals without their knowledge. As Custers and Vrabec (2024) pointed out, inferred predictions “may concern characteristics that people may not want to disclose about themselves (such as sexual orientation or mental health)” and in some applications, these may be “characteristics that people may not even know about themselves” (p. 5). Like the derived equity categories observed in Section 4.3—but particularly, low SES—they share with inferred data a problem, or challenge, of transparency, notice, and consent. In plain terms, equity group identification can be the output—inferences can be used to reveal equity, or equity-like, traits at scale and with little or no transparency. This was a central concern of the Australian Government’s recent review of the Commonwealth *Privacy Act 1988* (Attorney-General’s Department, 2022), which is returned to in Section 5.

Second, while machine-powered inferences can identify equity, or equity-adjacent traits, without a student’s knowledge, they can also leverage existing equity data—either derived characteristics or self-disclosed—for a variety of inferential purposes. This is to say, equity characteristics can be used as inputs. As mentioned above, those who design academic risk

profiling programs may choose to incorporate a student's equity characteristics as input data, within a predicative analytics process (Stephenson et al., 2022). Using traditional equity data categories as inputs for inferential processes raises significant ethics and governance concerns. We address these issues throughout this report, with detailed analysis in Sections 6.5.3 and 7.3.9.

The third point to stress about inferential data, both when it is used to identify or reveal equity characteristics (output), or when equity characteristics are used to power an inferential process (input), is the group or relational aspects of inference.

In fact, the ubiquity of digital data collection, when combined with powerful algorithmic inference, has also fundamentally changed how data about people are understood. As Viljoen (2021) argued, data in the digital age are not merely individual and descriptive but fundamentally relational. They are produced and utilised to generate inferences based on population-level patterns rather than solely on individual attributes. This creates new risks for equity groups that extend beyond direct data collection to include predictive classification and the repurposing of data across multiple contexts.

This relational dynamic is a central insight and concern of the Indigenous data sovereignty movement, both internationally and within Australia, which asserts the collective right of Indigenous peoples to govern the collection, ownership, and application of data concerning their communities (Rana & Azeez, 2025). These insights regarding the relational and collective nature of data about, and collected from, Indigenous peoples challenge Western conceptions of privacy, which typically centre on the individual. These principles are embedded in the *CARE Principles for Indigenous Data Governance*, in which the "C" (Collective) emphasises that Indigenous privacy relates to communal as well as individual privacy (Carroll et al., 2020).

In the domain of disability services and welfare, scholars and advocates have also drawn attention to the potentially harmful effects of algorithmic and inferential data practices. As van Toorn and Scully (2024) argued, such systems often reduce complex, relational experiences of disability to functional scores, producing both epistemic and material harms. These digital harms emerge when systems fail to account for the social and political contexts that shape need, and instead rely on narrowly defined, decontextualised data points.

4.4.5 Equity data as grey data

Taken together, these insights indicate that our understanding of student equity data must expand to include the volumes of digital data that are now routinely captured, linked, enriched, and leveraged to create inferences and algorithmically formed "unknowing collectives" to which individuals are assigned (Wong et al., 2024, p. 11). Therefore, the governance of equity data must now address new sources of value and risk, along with increasing technical and ethical complexity.

While recent discussions have rightly called for expanding data collections to include new equity groups, this analysis shows that the landscape of equity-related data is already much broader than is often acknowledged and extends well beyond the official group classifications represented by the Martin Indicators. To meaningfully embed equity within contemporary data and digital governance frameworks, a more expansive and complex terrain must now be reckoned with. This includes not only self-disclosed and administrative

data but also a range of often-unacknowledged data forms—incidental, third-party, behavioural, relational, and algorithmically inferred—all of which profoundly shape how students are seen, supported, and sorted.

The concept of grey data, as articulated by Borgman (2018), offers a useful lens for understanding this expanded equity data landscape. Grey data refer to the vast array of data collected through universities' routine academic, administrative, and service functions—such as data from LMS, student ID cards, library systems, and digital platforms. Much of these data are collected, stored, and deployed without formal institutional oversight because they are "difficult to identify or govern" (p. 371), yet they are increasingly used in ways that can influence high-stakes decisions about individuals and groups. As Borgman (2018) emphasised, grey data can be aggregated and repurposed to create inferred profiles or predictive classifications, often without the knowledge or consent of those affected.

These practices raise significant concerns about privacy, transparency, and accountability—particularly when equity-related inferences are derived from systems originally intended for administrative or educational functions. Understanding equity data today requires engaging with the often-hidden governance challenges posed by grey data, along with the inferences, privacy risks, and broader potential for data-related harms they entail.

*This mapping of systematic, incidental, indirect, and inferred ("grey") equity data underpins **R3** (national baseline and shared taxonomy or minimum controls), **R4** (privacy-by-design implementation—PIAs, model-risk, access or retention), and **R5** (harmonised treatment of third-party and local data across the policy suite), and motivates **R1** (life cycle guardrails in equity policy reforms).*

4.5 Equity data as risky data

Australian privacy law, beginning with the *Privacy Act 1988* (Cth) and reflected in state and territory law, has established a tiered approach to data protection. This framework distinguishes between two categories of information: "personal information" and the more stringently protected subcategory of "sensitive information". Although this report explores Australian data privacy law in greater detail in Section 5, this subsection introduces this fundamental distinction and highlights its significance to equity work as data work.

*This section motivates **R1** (life cycle guardrails in equity policy), **R3** (national baseline and shared definitions or controls), **R4** (risk-based, privacy-by-design implementation), and **R9** (profession-led practice standards and exemplars).*

4.5.1 "Personal" and "sensitive" data

Personal information is defined as any "information or opinion about an identifiable individual, or an individual who is reasonably identifiable" (*Privacy Act 1988* [Cth], s 6[1]). This classification is significant because it triggers a range of obligations under the Australian Privacy Principles (APPs)—the core set of legally binding rules or principles in the *Privacy Act*—regarding the collection, use, disclosure, storage, and security of such data, as well as individuals' rights to access and correct their information.

Any data that fail to meet the definition of “personal information” are subsequently not subject to the protections of the *Privacy Act.* This holds many important implications for student equity work as data work.

A key limitation of Australian privacy law is that its definition of personal information struggles to accommodate contemporary data practices. As a result, many forms of inferred or algorithmically processed data may fall short of this threshold, particularly if the link to an identifiable individual is not explicit. When data fall outside this definition—a category that includes successfully de-identified data—they also fall outside the privacy protections afforded by Australian law.

While these gaps in Australian privacy law have broad implications for equity work as data work, the primary focus on protecting individual privacy remains particularly salient. As Taylor (2020) argued:

> If understood narrowly, this approach risks failure to acknowledge the importance of data relating to multiple persons (group data) and its appropriate control within the framework of data governance. There is an increasingly urgent need to address this risk. (p. 730)

As seen in Section 5 of this report, the recent government review of the *Privacy Act* (Attorney-General’s Department, 2022) has gone some distance towards the recognition of these concerns, but it remains to be seen what changes government will ultimately adopt.

Rather than outline a general definition of sensitive information, the *Privacy Act* provides an exhaustive list of discrete information categories that are to be classed as sensitive and therefore receive greater privacy protections. These include personal information relating to:

- racial or ethnic origin
- political opinions or membership of a political association
- religious beliefs or affiliations
- philosophical beliefs or affiliations
- membership of a trade union or professional or trade association
- sexual orientation or practices
- criminal record
- health information
- genetic information
- biometric information and biometric templates.

Sensitive information is afforded heightened protection due to its potential to cause harm or discrimination if mishandled. Typically, this data relates to personal attributes for which discrimination is legally prohibited. This higher standard of protection is generally reflected across state and territory privacy legislation, although definitions and enforcement mechanisms can vary.

The implications of this classification are significant because organisations are subject to more rigorous requirements when handling sensitive information. Key protections for sensitive information are:

- *Strict collection rules (APP 3):* Unlike the collection of personal information, sensitive information can generally only be collected directly from an individual and with their explicit consent.

- *Notification requirements (APP 5)*: Organisations must provide a privacy collection notice that clearly informs individuals, at or before the time of collection, of the specific purpose for which sensitive information is being gathered.
- *Limitations on purpose and use (APP 6)*: The use and disclosure of sensitive information are heavily restricted and typically cannot be used or disclosed by an organisation for any purpose other than the one for which it was collected unless a specific legal exception applies.
- *Strict security requirements (APP 11)*: Organisations collecting and handling sensitive information are required to take extra steps to protect it from misuse, loss, or unauthorised access.

Applying these sensitive information classifications to commonly recognised higher education equity groups reveals both variation and contextual ambiguity. While all equity group information that can be identified with a person meets the standard of personal information, its classification as sensitive information is less straightforward.

Both First Nations status and a student's disability status clearly fall under the definition of sensitive information, aligning with the categories of "racial or ethnic origin" and "health information" respectively. In contrast, information relating to students from low SES backgrounds or regional or remote areas would typically be classed only as personal information. This is not to say, however, that data relating to low SES or regional or remote group classifications should be considered lower risk in all contexts. Considerations of risk are returned to in Section 4.5.3.

4.5.2 Is equity data sensitive data?

While the classification of core equity groups such as First Nations students and students with disability is relatively straightforward, the picture becomes less clear for the many other "unofficial", proposed, or legacy equity cohorts. Of these, information relating to a student's status as a current or former prisoner is perhaps the only group to clearly fall under the sensitive classification via the protected category of "criminal record". The classification for other unofficial equity groups, however, carries varying levels of ambiguity and contextual nuance.

For example, students from NESBs—a term now largely replaced by the definitionally distinct category of culturally and linguistically diverse backgrounds—may in some instances be judged to intersect with or imply information relating to "racial or ethnic origin", "political opinions", and "religious beliefs". Information relating to a country of birth or languages spoken at home can, in some circumstances, act as proxies for a person's "racial or ethnic origin", which is explicitly categorised as sensitive.

Similar concerns may be raised for data relating to students from refugee and Pasifika backgrounds. A student's refugee status, for example, may reveal "racial or ethnic origin" or "political opinions"—relevant in cases of persecution—both of which are categories of sensitive information. Likewise, information about Pasifika students, although a rich and nuanced term (Australian Pasifika Educators Network, 2023), would likely be classified as sensitive information if it were judged to pertain to "racial or ethnic origin".

The privacy protections afforded to gender identity data under Australian law are more limited than might perhaps be widely appreciated. The *Privacy Act* does not include gender

identity as a category of sensitive information. Protection for such data at the Commonwealth level depends instead on whether it can be characterised as health information, or whether it can be inferred from a listed category such as sexual orientation or practices. Neither of these provides a reliable or consistent basis. Western Australia has moved to resolve this gap explicitly: the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act) explicitly lists both gender identity and sexual orientation as discrete categories of sensitive personal information.

This complexity surrounding gender data classification is increasingly salient given the Department of Education's recent changes to the "E315 Gender" code in TCSI. As of January 2026, this updated code will become part of mandatory reporting and will include the following values for students and staff to choose from:

- F – Female/Woman
- M – Male/Man
- N – Non-binary
- D – Different term
- P – Prefer not to answer.

This update aligns TCSI gender data collection with the Australian Bureau of Statistics' (ABS, 2020) *Standard for sex, gender, variations of sex characteristics and sexual orientation variables*, moving beyond a simple male/female binary. These new data categories almost certainly warrant treatment as sensitive, yet their status under Commonwealth law remains ambiguous. This matters particularly for practitioners and researchers constructing intersectional datasets, such as those seeking to evaluate program effectiveness for gender-diverse students. In doing so, they may be working with information that carries significant re-identification and discrimination risks, regardless of whether it formally meets the threshold for sensitive information under the *Privacy Act*.

Proposed equity groups such as student veterans and care leavers generally fall outside the statutory definition of sensitive information in Australian law. Yet data gathered to understand their circumstances or provide support often involve or reveal sensitive details—for example, a veteran's health condition or a care leaver's history of personal hardship. Beyond such incidental disclosures, the relational nature of data, as seen in Section 4.4.4, means that group identifiers can themselves imply sensitive attributes (Viljoen, 2021). A similar dynamic applies to carers (or caregivers): identifying a student as a carer may expose another person's health information. Accordingly, a student's carer status is best treated as sensitive health information, although few university policies make this explicit (see Section 6).

4.5.3 Towards a risk-based approach

A two-tiered data protection model that hinges on rigid, exhaustive lists of "sensitive" categories is increasingly unfit for the digital age and creates significant protection gaps. As Solove (2023) argued, this approach is fundamentally flawed because it embraces the idea that the appropriate legal protection can be determined simply by looking at the nature or content of the data, rather than its context, use, or potential for causing harm. Solove (2023) identified three core failures that are relevant here:

- *Arbitrary classification and blurred boundaries*: The approach attempts to simplify complexity by deeming certain data categories sensitive, yet this shortcut is thin on logic and often fails to achieve clarity (p. 1111).
- *Inference power*: The sensitive data categories are easily undermined by modern data analytics because non-sensitive data can readily give rise to inferences about sensitive data. Consequently, “nearly all personal data can be sensitive, and thus the sensitive data categories can swallow up everything” (p. 1099).
- *Misplaced protections*: This approach ignores situations in which non-sensitive data causes significant harm while mechanically elevating certain trivial harms for heightened protection (p. 1111).

This conceptual failure underpins the view that privacy protection should not be determined mechanically according to exhaustive lists; instead, it should be proportionate to the potential harm and risk posed by the data’s collection, use, and disclosure. A risk-based approach, according to Solove (2023), shifts the focus from what the data are to what the data do, requiring organisations to proactively assess the likelihood and gravity of harm in each context.

Risk is especially acute in equity work, in which the very characteristics that define equity groups—disadvantage, under-representation, and heightened vulnerability—necessitate the routine collection and handling of sensitive attributes (for example, disability, Indigenous status, low SES, regionality) across multiple systems and teams. If those data are overcollected, poorly secured, or repurposed for predictive analytics, students can face serious harms: privacy breaches, stigma and profiling, chilled engagement with support services, and downstream discrimination in academic or administrative decision-making (Prinsloo et al., 2024b).

To address these legal shortcomings, organisations with robust data governance policies typically supplement the categorical tiers of “personal” versus “sensitive” information by adopting or developing their own, more granular, risk classifications (Andersson, 2023; Nguyen & Cuong, 2025). Under these more nuanced, risk-based classification systems, data that do not meet the legal threshold for “sensitive” information may still be classified at an equivalent level of risk if they carry the potential to cause harm. In this way, an organisation’s internal classification system should serve to implement a more comprehensive and ethical approach to privacy that extends beyond the strict letter of the law.

Internal risk classification is also a practical lever for demonstrating compliance with the APPs. Specifically, APP 11 mandates that organisations take “reasonable steps” to protect personal and sensitive information, which includes limiting internal access on a need-to-know basis. By proactively designating certain datasets, or data types, as higher risk—even if they do not meet the legal definition of “sensitive” information—institutions can effectively justify and enforce tighter technical and administrative controls, such as granular access permissions, stringent provisioning, access logging, and regular audits. This approach provides demonstrable evidence of meeting the “reasonable steps” standard, thereby reducing both legal and reputational exposure.

In fact, many Australian universities have now adopted nuanced information security and risk classification systems as a core governance strategy. However, these frameworks remain difficult to implement and carry a host of inherent challenges.

4.5.4 Critical limitations of risk classification

Data-risk classification schemes are widely recognised as a hallmark of organisational information security, but in practice they face persistent and fundamental limitations (Andersson, 2023). For universities managing sensitive student equity data, these weaknesses create particularly acute governance challenges.

A recurring difficulty is deciding on the appropriate level of granularity. As Andersson (2023) explained, highly detailed classification can overwhelm staff and resources, while broad, system-level categories risk leaving critical assets unidentified (p. 454). For universities, classifying all “student records” as a single category can obscure the distinctive vulnerabilities of equity-related data such as disability or First Nations information.

Conversely, attempting to classify every individual record is impractical at scale. Equally, many organisations struggle to maintain a complete and current registry of information assets, which is essential for effective data classification and protection. In the higher education context, equity data are often scattered across student management systems, analytics platforms, and disability support records, making it difficult to build a comprehensive inventory. This fragmentation of grey equity data increases the risk that sensitive datasets are overlooked in risk assessments, leaving them unprotected.

Yet the most serious limitations are not technical but human and institutional. Andersson (2023) highlighted how classification activities are shaped by subjective judgements because different actors bring their own values, assumptions, and professional perspectives to the same data (pp. 456–457). This results in inconsistent or overly cautious classifications. In universities, the diversity of roles involved in handling equity data—IT staff, academic leaders, administrators, and frontline equity practitioners—amplifies this subjectivity.

These divergent risk judgements emerged strongly in the interviews, particularly among staff in disability support units (see Section 7). The result is uneven thresholds for what counts as “high risk”, ad hoc access decisions, and a pronounced drift between policy and practice. Because this subjectivity undermines efforts to build a coherent, organisation-wide classification and governance approach, it remains one of the most significant weaknesses of current risk schemes.

Finally, problems of communication and interpretation further compound these issues. Andersson (2023) showed that even when classification frameworks are in place, their language is often vague, technical, or inconsistent, and terms such as “confidential” or “high impact” are interpreted differently across departments (pp. 457–458). Generic standards are also difficult to adapt to local institutional contexts, leaving staff to rely on guesswork or informal practices.

In student equity data, this contributes to a dual risk: overprotection, through which restrictions limit the appropriate use of information for student support and inclusion; and underprotection, through which gaps in practice leave students vulnerable to harm through breaches or misuse. Together, these limitations underscore that classification systems, while essential in theory, are fragile in practice—and that their shortcomings are especially consequential when applied to sensitive equity data in universities.

4.6 Whose risk? Whose decision?

As shown more concretely in Section 7, equity data work distributes risks and benefits across students, staff, and institutions. A relational lens acts as a reminder that these effects extend beyond the university, because the risks of equity data are collective, not merely individual (Viljoen, 2021). The legitimacy of a data governance program therefore turns on how decisions about data are made and who is represented in decision-making processes. At the same time, data-risk classification schemes are fragile when deployed in "the grey" of professional practice: choices about granularity, incomplete inventories, subjective judgements, and generic standards routinely miss the mark. In this light, governance of student equity data cannot rely on getting categories "right" in advance (Andersson, 2023). While data-risk classifications are part of the data governance solution, their practical impact remains limited.

Nor is the answer simply to push finer-grained privacy controls onto individual students. The individual-control model again represents only a partial fix. As discussed further in Section 5, the individual-control model of privacy management struggles on two fronts: (i) it overburdens students with frequent, technical choices in complex systems, rendering "consent" largely symbolic and ineffective; and (ii) it cannot govern the collective and institutional effects of equity data (for example, cohort-level treatment, allocation decisions, downstream sharing) that extend beyond any one person's preferences (Manwaring et al., 2021; Solove & Hartzog, 2024). As Moses and Weatherall (2024) forcefully argued, "privacy is a collective good: *my* privacy (what people can know and infer about me) depends on *your* actions (what information *you* choose to disclose *about you*)" (emphasis in the original, p. 9). The upshot, as Solove and Hartzog (2024) argued, is that law and governance should constrain organisational practices rather than outsource responsibility to individuals.

Because equity data risks are shared decisions about a university's equity data, collection, management, and use should be co-designed with those who bear the risks and those who steward the data day-to-day (Jarke & Büchner, 2024). This serves to highlight the pressing need for participatory and democratic equity data governance mechanisms within universities (Dollinger & Lodge, 2019; Stephenson & Harvey, 2022; Swist et al., 2024). For example, standing equity data governance forums with representation from students (including disability, First Nations, and other equity cohorts), equity practitioners, academic and professional staff, and data governance, privacy, or security specialists. This brings decision-making closer to affected communities, builds legitimacy, and provides a workable way to adapt as values, technologies, and practices change—without shifting responsibility onto individual students.

*Section 4 expands what counts as student equity data (official, incidental, indirect, inferred, and grey) and surfaces associated risks—motivating **R1** (life cycle guardrails), **R3** (national baseline with shared taxonomy and minimum controls), **R4** (privacy-by-design, risk-based PIAs and ADM transparency), **R5** (harmonised treatment across the policy suite), and **R9** (profession-led practice standards and exemplars).*

5. Australia's privacy legislation framework: "Outdated and unfit"

The aim of Section 5 of this report is to outline the changing legislative and regulatory landscape that frames the broader context for equity data governance in Australian universities. This framing leads into the first research question (RQ1), which focuses on macro-level data and digital governance:

> **(RQ1):** What are the current and emerging legislative and regulatory frameworks for data privacy in Australia, and how might pending reforms affect universities and the governance of student equity data?

This section outlines the macro-level legislative and regulatory context shaping equity data practices in Australian public universities. In addressing RQ1, the focus is specifically on recent and proposed changes to Australian data privacy law that are likely to reshape the environment in which equity data work takes place.

It is significant to consider that Australia's foundational privacy law—the *Privacy Act 1988* (Cth)—was introduced just two years before *A Fair Chance for All* (1990) established our enduring equity framework. Each was established well before "big data", AI, and sophisticated analytics fundamentally changed the data landscape, creating new privacy risks and digital challenges, but also opening fresh opportunities to more effectively identify and address equity needs.

While the Accord has underscored the urgent need to modernise Australia's higher education equity framework—which has remained largely unchanged for over 35 years—a parallel effort is now well underway to reform the nation's privacy laws in response to a vastly transformed digital landscape. In 2020, the Australian Government initiated a comprehensive review of the ageing *Privacy Act*. The terms of reference for the *Privacy Act Review* stated:

> As Australians spend more of their time online, and new technologies emerge, such as artificial intelligence, more personal information about individuals is being captured and processed raising questions as to whether Australian privacy law is fit for purpose. (Attorney-General's Department, 2022, p. 311)

The *Privacy Act Review Report 2022* was publicly released in February 2023 and contained 116 proposals for the modernisation of the federal *Privacy Act*. The government's response to the report was released in September 2023, indicating it "agreed" to 38 proposals, "agreed in-principle" to 68, and the remaining 10 proposals were "noted" (Australian Government, 2023). In a speech given the following year, Attorney-General Mark Dreyfus further detailed the government's position on the need for reform:

> the Privacy Act, which is the primary vehicle for regulating personal information of Australians, is *woefully outdated and unfit for the digital age*. The speed of tech innovation and the rise of artificial intelligence underpins the need for legislative change.

> It is clear that personal information has immense value—not just to individuals, but to those engaged in marketing, research, product development and advertising.
>
> *But the Privacy Act framework dates back to the 1980s and is not fit for purpose for our modern economy.* It's past time we stopped treating the most personal and private information of Australians as an asset that entities hold. (Dreyfus, 2024, emphasis added)

The "first tranche" of legislative reform was first realised through the *Privacy and Other Legislation Amendment Act 2024* (Cth), which was introduced to Parliament in late 2024 and took effect on 10 December 2024. The reforms addressed just 23 of the *Privacy Act Review*'s proposals, but a "second tranche" is expected to address many more.

Before discussing the major points of recent and pending reform, it is important to note how these reforms may affect—or, indeed, fail to affect—university privacy practices across the sector.

5.1 A fragmented privacy framework

Some Australian sectors operate under specific federal privacy codes or dedicated regulatory frameworks—credit reporting and the My Health Record system are notable examples. Universities, by contrast, do not operate under any equivalent sector-wide privacy code under the *Privacy Act*. This contrasts with regions such as the United Kingdom and the European Union, where the *General Data Protection Regulation* (EU) and *UK General Data Protection Regulation* impose standardised, world-leading data protection obligations across the higher education sector. The absence of a sector-specific federal privacy framework contributes to an important measure of variability in privacy protections for students and complicates institutional compliance across the higher education sector.

Australia's privacy legislative framework has long been recognised, and lamented, for its "multi-layered, fragmented and inconsistent" nature (Australian Law Reform Commission, 2008, p. 190). As Rule and Greenleaf (2010) colourfully explained:

> Australia's very boring history, constitutional structure, and legal history provides much of the explanation of why privacy is protected in Australian law principally by a patchwork of specific legislation. (p. 148)

"Boring" or not, this "patchwork" of privacy law has created a complex environment for public universities, and those who work within them, as they strive to responsibly collect, manage, and utilise student data.

Among the Table A providers (see Appendix Section 10.1 for the list), only a small number are subject to the *Privacy Act 1988* (Cth) as a core, institution-wide privacy framework. The Australian National University (ANU) is the clearest example: as a Commonwealth statutory authority established under the *Australian National University Act 1991* (Cth), it is governed by the *Privacy Act* as an "agency" for the purposes of that Act.

Two further Table A universities are also more directly governed by the *Privacy Act* because of their legal structure. Australian Catholic University (ACU) and the University of Notre Dame Australia (UNDA) are not established as state public universities in the same way as most other Table A providers. ACU is incorporated as a public company limited by guarantee

and is subject to the *Corporations Act 2001* (Cth). UNDA, although established under Western Australian legislation, operates nationally as a private Catholic university. In practical terms, both institutions are treated as APP entities for *Privacy Act* purposes and must comply with the APPs as a central part of their institutional privacy obligations.

This places ANU, ACU, and UNDA in a structurally distinct position relative to the majority of Table A universities, which are state or territory public bodies primarily governed by their respective state or territory privacy legislation. Most Australian public universities operate under two layers of law: limited obligations under the *Privacy Act* arising from specific federally mandated contexts such as HESA and TCSI reporting, tax file number handling, and Commonwealth contracts, with primary governance sitting under state or territory privacy legislation. Some states and territories have enacted dedicated privacy legislation for this purpose; South Australia has established an administrative framework rather than a legislative one. ANU, ACU, and UNDA, by contrast, are governed primarily and comprehensively by the Commonwealth *Privacy Act*. While state and territory privacy laws are generally aligned with the core principles of the Commonwealth Act, significant legislative fragmentation remains, creating complexity and varying protection standards across Australian jurisdictions.

Legislative fragmentation is particularly evident concerning health information, including data students provide when disclosing disability and related medical documentation. Certain jurisdictions have enacted dedicated health privacy statutes—such as the *Health Records and Information Privacy Act 2002* (NSW) and the *Health Records Act 2001* (VIC)—which establish specific requirements for managing health-related data. These specialised statutes coexist alongside broader state or territory privacy laws, creating overlapping obligations that universities must carefully navigate.

Although the *Privacy Act* has particular significance for ANU, ACU, and UNDA, it also significantly influences privacy practices across the wider higher education sector. Notably, all Table A providers must comply with the APPs in particular HESA contexts. Section 19-70 of HESA requires higher education providers to give the Minister specified statistical and other information, while s 19-60 requires APP compliance for personal information obtained for specified HESA purposes. These obligations are significant for TCSI reporting, including student demographic and equity-related data reported to government.

Importantly, several Australian universities, but particularly those in jurisdictions with less robust privacy legislation, have voluntarily adopted the higher standards set by the *Privacy Act* and apply them more widely across the organisation. This voluntary adoption of the *Privacy Act* is further explored in Section 6.

In sum, even where the *Privacy Act* does not apply in a uniform and sector-wide fashion, its standards substantially shape universities' policies, procedures, and day-to-day data practices. Nevertheless, this layered legislative complexity highlights the practical challenges universities face in establishing clear and consistent data privacy and governance practices. From a macro-level perspective, there remain significant areas of legal and ethical ambiguity, or "grey zones", that institutions must carefully navigate.

5.2 Reforming Australia's privacy framework

Having outlined the fragmented nature of Australia's privacy framework, this section turns to the Australian Government's formal review of the *Privacy Act*, which produced 116 reform proposals (Attorney-General's Department, 2022). The discussion focuses on those proposals most relevant to the governance of student equity data in higher education. While it is recognised that *Privacy Act* reforms may not directly or immediately apply across the higher education sector, it is useful to consider their implications for student equity data and digital governance for at least two reasons. First, debates emerging from the *Privacy Act Review* offer valuable insights into broader shortcomings of Australian privacy law, helping to clarify the ambiguities—or grey zones—within the current framework.

Second, although states and territories are not required to adopt the Commonwealth standards, changes to federal law often encourage movement towards harmonisation. Indeed, the *Privacy Act Review Report* explicitly recommended establishing a "Commonwealth, state, and territory working group to harmonise privacy laws, focusing on key issues" (Attorney-General's Department, 2022, p. 302), a recommendation to which the government has "agree[d] in-principle" (Australian Government, 2023, p. 38).

It is also important to note that state and territory privacy legislation is not always less stringent or protective than the federal *Privacy Act*. For example, Western Australia, like South Australia, recently lacked a dedicated privacy act but has now enacted the PRIS Act, which—in certain key respects—is more demanding than the federal Act. Specifically, the PRIS Act introduces mandatory privacy impact assessments (PIAs), explicit transparency and oversight requirements for automated decision-making (ADM), and innovative protections for Aboriginal and Torres Strait Islander data governance. Given that the PRIS Act received Royal Assent in December 2024, scholarly evaluation and analysis of its practical impacts remain limited at the time of writing.

Reform status note: The following subsections examine key areas of proposed reform to the *Privacy Act* that are particularly relevant to the governance of student equity data. Each of these reforms, including changes to consent standards, definitions of personal and sensitive information, and fairness requirements, have been agreed or agreed in principle by the Australian Government but have not yet been enacted at the time of writing. They are expected to be introduced in a second legislative package (Tranche 2) as part of a broader modernisation of Australia's privacy framework. While the *Privacy Act* does not apply uniformly across all universities, this report recommends that all institutions commit to adopting these updated standards as they come into force, regardless of their formal legal obligations. If enacted, these new standards may help universities cut through a substantial amount of the grey for both students and staff.

5.2.1 Modernising definitions of "personal" and "sensitive" information

Section 4 examined how Australian privacy law distinguishes between personal and sensitive information. It also noted that while categorising equity group data within this hierarchy is not always straightforward, whether sourced from direct self-disclosure or from derived and inferred statuses, the task remains important. Section 6 returns to this issue by examining university policies for evidence that such determinations have been made and, importantly, whether they have been made transparent.

The *Privacy Act Review Report* (Attorney-General's Department, 2022) exposed a significant limitation in Australia's privacy legislation, deeming its current understanding of personal and sensitive information too individualistic and outdated for the complexities of the digital era. The definition of "personal information" is fundamental because it delineates the scope of the *Privacy Act* itself. In simple terms, if information does not meet the definition of personal information, then the obligations set out in the APPs—such as rules about collection, use, disclosure, security, and an individual's access rights—generally do not apply.

Personal information is currently defined by the *Privacy Act* as "information or an opinion *about an identified individual*, or an individual who is *reasonably identifiable*" (s 6, *emphasis added*). Recent critiques of the Act have underscored that its existing definition of personal information is ill-suited to contemporary data practices, particularly because new technologies enable the generation of vast amounts of data about individuals, including through inferences and technical means, often without direct identification of individuals in the traditional sense (Moses & Weatherall, 2024). This has led to calls for significant reform because the current framework creates uncertainty about whether such data fall within the Act's scope, potentially leaving significant areas of data processing unregulated.

In response to these shortcomings, the *Privacy Act Review Report* (Attorney-General's Department, 2022) aimed to broaden the scope of personal information and enhance clarity. Key recommendations include amending the definition of personal information to cover data that "relates to" an individual, explicitly encompassing technical and inferred information (Attorney-General's Department, 2022, Proposal 4.1, p. 25; Proposal 4.3, p. 30). Furthermore, the narrower category of sensitive information, which demands higher privacy protections, would be clarified to confirm that sensitive attributes can be inferred from non-sensitive data (Attorney-General's Department, 2022, Proposal 4.9.c, p. 45).

Crucially, these reforms aim to clarify legal grey zones by arguing that technical or inferred data do, in fact, constitute "personal information", thereby expanding the practical application of privacy safeguards to a broader range of digital information. If the proposals were adopted or applied to universities, the modernised definitions would clarify that a wider range of student data—including insights generated through learning analytics, and inferred characteristics—falls within the scope of privacy law.

5.2.2 Strengthening notice and consent requirements

Effective privacy protection relies on individuals being adequately informed before or at the time their data are collected. Australian privacy law addresses this through two key mechanisms: an institution's general or central privacy policy (governed by APP 1 of the *Privacy Act*), which outlines the overall personal information management practices of an institution (or entity); and the more specific privacy collection notice (governed by APP 5), which must be provided to an individual for a particular instance of data collection. The *Privacy Act Review Report* (Attorney-General's Department, 2022) emphasised that these two instruments, general policies and collection notices, serve distinct functions:

> An APP 1 privacy policy is necessary at all times and covers the entity's entire personal information handling practices. It facilitates monitoring of compliance and is valuable for particularly concerned individuals, civil society groups, researchers or regulators. On the other hand, APP 5 collection notices, when required, should be

> concise, easy for the average consumer to understand, and should only contain information that is relevant to the particular collection of personal information. (p. 95)

The review also acknowledged concerns that current collection notices are often too long, complex, and difficult to understand, thereby undermining genuinely informed choices.

Against this backdrop, proposed reforms from the *Privacy Act Review Report* (Attorney-General's Department, 2022) aim to raise the standard for consent, requiring it to be voluntary, informed, current, specific, and expressed through unambiguous affirmative action (Proposal 11.1, pp. 102–105). Within universities and other institutional settings, consent for data collection and use is often not obtained in a sufficiently meaningful or detailed manner that reflects the sensitivity of the data involved. Instead, it is frequently bundled into general terms accepted at enrolment or inferred through students' use of institutional systems. This practice reflects what scholars call "murky consent" (Solove, 2024), where the conditions for truly informed and specific agreement are undermined by lengthy notices, vague consent mechanisms, and power imbalances between institutions and students who must access essential services.

While "murky consent" practices stem from both macro-level legislation and meso-level institutional policies, interview participants in this Fellowship project frequently expressed concern that universities are not doing enough to secure fully informed consent from students across various data uses. These concerns are explored further in Section 7.

The proposed standard for consent as an "unambiguous indication of their wishes through clear action" (Attorney-General's Department, 2022, Proposal 11.1) would likely render silence (inaction), pre-ticked boxes, or default opt-ins insufficient. Valid consent would require a clear, positive act—such as clicking "I agree" after a specific explanation or adjusting user settings (Attorney-General's Department, 2022, p. 105). This shift prioritises clarity and individual choice, and if enacted, universities would need to ensure that privacy notices—but particularly those relating to TCSI data collections under HESA—include clear, specific notices about statutory collections and provide active consent where consent is the lawful basis.

The focus on improving consent standards rests on the assumption that students can make meaningful choices about how their data are used. However, consent is often constrained by institutional settings where participation is not truly optional. Students cannot easily refuse to provide personal information without compromising their access to essential services, such as enrolling in courses, receiving support, or using digital learning environments. In many cases, the only real alternative to consenting is to disengage from the university altogether.

This raises a deeper concern: even if consent becomes more "informed" or "unambiguous", it may still fail to protect individuals from unfair data practices, but particularly when those practices are embedded in non-negotiable systems. Recognising this, the proposed reforms introduce an additional safeguard—the "fair and reasonable" test.

5.2.3 The "fair and reasonable" test

A notable proposed reform to the *Privacy Act* is the introduction of a requirement that personal information be handled in a manner that is "fair and reasonable" in the circumstances (Attorney-General's Department, 2022, Proposal 12.1). This test shifts the focus from formal compliance—such as simply obtaining consent—to assessing whether

data practices are substantively justifiable considering their context, risks, and potential impacts. Crucially, it addresses a major grey zone in current Australian privacy law: situations in which consent may have been obtained, but the resulting data use remains ethically questionable or overly intrusive.

Designed to operate as a critical backstop, the fair and reasonable test ensures that organisations cannot rely solely on consent to justify such practices. As Kemp (2023) argued, this reform "recognises consumers' severely limited ability to understand data practices and their consequences, and the additional obstacles to consent posed by organisations' control of the choice architecture" (p. 5). For universities, this would necessitate a fundamental change in approach: moving beyond simply asking "Did the student agree?" to rigorously assessing whether a specific use or disclosure of student data is appropriate, truly necessary, proportionate to any benefits, and respectful of student expectations and welfare.

The test would also reinforce proportionality in data practices. For example, even where data use is permitted, institutions may need to consider whether that use is necessary, reasonable, and likely to meet students' expectations. In analytics and profiling scenarios, this could involve asking not just "Did the student agree?" but also "Is this appropriate?" This new safeguard fills a critical regulatory gap, ensuring accountability for data practices that previously fell outside clear legal scrutiny, even if technically compliant.

5.2.4 Enhanced transparency in automated decision-making

Recognising the increasing use of automated systems to make decisions with significant consequences for individuals, the *Privacy Act Review Report* (Attorney-General's Department, 2022) put forward specific proposals to enhance transparency in ADM. These proposals aim to ensure individuals are better informed about such practices and better able to contest them. This direction aligns with European Union law: the EU *Artificial Intelligence Act* automatically classes the use of ADM systems in educational contexts as high risk. While the Australian proposals have not yet adopted this high-risk threshold for ADM, they represent a clear step towards better regulatory alignment.

Two key proposals from the review directly address ADM transparency. Proposal 19.1 recommends that APP entities be required to disclose in their privacy policies "the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights" (Attorney-General's Department, 2022, p. 191). Proposal 19.3 introduces a right for individuals to request meaningful information about how such decisions are made and further reinforces the need to include this information in privacy policies (Attorney-General's Department, 2022, p. 193).

Importantly, the review does not propose giving individuals the right to opt out of ADM processes or request human review of decisions (Attorney-General's Department, 2022, p. 193). However, other relevant provisions would still apply, including the proposed "right to object" to data handling (Attorney-General's Department, 2022, Proposal 18.2, agreed in principle) and the broader "fair and reasonable" test (Attorney-General's Department, 2022, Proposal 12.1). The Australian Government (2023) "agreed in-principle" to both transparency-focused proposals, signalling an intent to legislate them following further consultation on implementation. If applied to universities, the impact of these reforms could be substantial.

The proposed measures target ADM systems that have a “legal or similarly significant effect” on individuals (Attorney-General’s Department, 2022, Proposals 19.1, p. 191). In a university context, this might be considered to include systems that significantly influence admissions decisions or academic progression monitoring that triggers major interventions. Certain learning analytics tools may also meet this threshold if their outputs are used to make largely automated decisions that materially affect students’ access to educational opportunities or support.

If adopted, both in legislation and by universities, the proposed reforms would require institutions to update their privacy policies to clearly disclose the use of student personal information in ADM systems that carry legal or similarly significant effects. Universities would also need to strengthen their internal understanding and documentation of these systems, provide “meaningful information” upon student request, establish clear procedures for handling such requests, and conduct audits to identify ADM processes that require enhanced transparency. Collectively, these agreed in principle reforms would promote greater accountability in universities’ use of ADM for student-related decisions and are likely to contribute to building student trust.

5.2.5 From fragmentation to reform: Embedding privacy-by-design

In sum, while the reform of Australia’s privacy laws remains a work in progress, the direction of change is clear: institutions are expected to move beyond minimal compliance towards more principled, proactive, and rights-respecting models of data governance. One of the most significant contributions from the Office of the Australian Information Commissioner (OAIC, 2023b) in this space is the endorsement of “privacy-by-design”—an approach that embeds privacy considerations into the architecture of systems, policies, and organisational practices from the outset.

Rather than treating privacy as a reactive obligation or technical add-on, privacy-by-design emphasises anticipatory action, student-centred safeguards, and ethical foresight. As the sector responds to rising expectations and increasingly complex data environments, adopting privacy-by-design will be critical for building trust, ensuring compliance readiness, and aligning data governance practices with the equity commitments that remain foundational to Australian higher education.

Sections 6 and 7 of this report build directly on this foundation, examining how institutional policies and frontline practitioner experiences reflect, and often struggle to meet, the regulatory expectations examined above.

*Section 5 summarises the changing legislative and regulatory landscape (definitions, consent, the “fair and reasonable” test, ADM transparency, privacy-by-design), underscoring the need for **R1** (policy life cycle guardrails), **R3** (national baseline with shared definitions or tools), **R4** (above-minimum, privacy-by-design implementation), and **R5** (harmonised institutional policies).*

6. University data and digital governance policies through an equity lens

In an era when Australian universities are navigating a deluge of student data and rapidly evolving digital technologies, the policies these institutions create are more than just administrative documents; they are crucial statements of intent, practice, and values. These policies act as the primary guideposts for managing sensitive, or high-risk, student information and ensuring that digital tools align with institutional missions. In attending to this meso level of institutional or organisational governance, the research question (RQ2) posed now is:

> **(RQ2):** How do Australian universities approach data and digital governance in their policies, and to what extent do these frameworks consider or prioritise student equity?

Understanding these university-level policies is vital because they translate complex external laws and regulations into daily operational procedures, striving for internal consistency and, ideally, providing transparency. While common threads emerge across the sector, significant differences also highlight each institution's unique approach and priorities in this critical domain.

Indeed, clear institutional policies are essential. The *Higher Education Standards Framework (Threshold Standards) 2021* (HESF) requires universities to demonstrate effective governance arrangements, including policies and procedures that ensure academic quality, institutional integrity, and accountability across their operations. Policies also serve as a critical transparency mechanism. For example, institutions use privacy policies to meet their obligations under the *Privacy Act*, and similar state and territory laws, by informing individuals of how their personal information is handled (OAIC, n.d.-a, n.d.-b).

This section presents a desktop review of the institutional data and digital policy landscape within and across Australian universities. The analysis presented for the purposes of this report primarily targets three policy categories: privacy policies, disability policies, and data or information governance policies. These categories were selected to offer comprehensive insight into university approaches to data and digital governance, particularly concerning student equity, while ensuring a focused and manageable scope for the inquiry, thereby preventing an overly broad investigation. Section 6 concludes with a high-level summary of findings on university Support for Students Policies (SfSPs), illustrating some of the challenges that arise at the intersection of data and digital governance.

6.1.1 Brief literature review

While research into AI governance in higher education is growing, comprehensive studies on broader data and digital governance frameworks at the (meso) institutional level, particularly

within Australian universities, are notably scarce. This literature gap underscores the necessity of the present study.

Existing research, although limited, suggests that the Australian higher education sector is still maturing its data and digital governance practices. In a recent study, Selvaratnam et al. (2024) surveyed Australasian higher education institutions to understand the maturity of their AI and data governance. In the domain of data, a majority, “59% felt they had up-to-date policies and guidelines and consistent adherence to industry and sector ethical practices by staff, both at the individual and team levels” (p. 3). This contrasts with AI, concerning which most institutions are still at the “experimenting and exploring” stage, highlighting a disparity in the developmental progress between data and AI governance within the sector (Selvaratnam et al., 2024, p. 1).

The recent study by McNicol et al. (2024) further indicated that Australian higher education data governance policies and practices appear to be in a developing stage, facing challenges in achieving full maturity and consistent application. The authors asserted that, more broadly, “No actionable framework is currently available in the country to govern the ethical usage of corporate data” in higher education (McNicol et al., 2024, p. 2247). This contrasts with the situation in the UK, where, for example, Jisc’s higher education data (governance) maturity framework has been widely adopted (Jisc, 2024).

Illustrating these sector-wide challenges at an institutional level, McNicol et al. (2024) found that in one Australian university, where a data governance framework had been developed, “awareness and implementation of this varied across the university” (p. 2267). Consequently, data sharing often occurred “on an ad hoc and individual basis”, and there was a notable “absence of a documented process for secondary uses of data” or for approvals across different information domains (McNicol et al., 2024, p. 2256).

Taken together, both studies suggest that while the Australian higher education sector is actively engaging with data and digital governance, both its frameworks and the cultures that support them are still maturing. Even when robust institutional policies exist, inconsistent awareness and implementation can leave personal and sensitive data inadequately protected.

*This framing supports **R5** (harmonise the policy suite), **R4** (privacy-by-design in practice), and **R3** (sector baselines aligned to the OAIC).*

6.2 Desktop review methodology

This study employed a desktop policy content analysis to examine how Australian universities approach data and digital governance through institutional policy, with particular attention to the integration of equity considerations. The review encompassed all 39 public universities classified as “Table A” providers under HESA (Compilation No. 92, January 2024). A full list of institutions appears in Appendix Section 10.1.

Only documents available in public-facing university policy libraries were included. Between March and May 2024, a systematic scan of each institution’s library was conducted using keyword searches to locate policies addressing privacy, data and information governance, learning analytics, cohort monitoring, AI, student success and support, and student equity.

Policies relating directly to students with disability and First Nations Australian students were also prioritised.

This process generated a pool of over 800 policy, procedure, and guideline documents which were grouped into approximately 30 policy types. A subsequent review and close reading identified policy categories most relevant to RQ2, including privacy, data and information management or governance, disability, equity, research, support for students, student success and retention, academic progression and monitoring, student cohort monitoring, AI, and learning analytics.

To balance breadth with depth, the in-depth analysis concentrated on four categories that provide a robust lens on the intersection of data, digital, and equity: privacy policies, data or information governance policies, disability policies, and SfSPs.

A small number of First Nations-specific policies focused mainly on identity protocols and cultural recognition (that is, not engaging directly with data governance or digital equity) were excluded, as well as most academic integrity policies and institutional statements addressing GenAI. Over 2024, these materials largely remained advisory rather than formal policy or guideline; sector-wide summaries are available in TEQSA (2024).

Although this review focused on publicly accessible content, several relevant artefacts—particularly in privacy, data governance, and information security—were listed in policy libraries but were not publicly available (for example, restricted data governance frameworks, internal data-handling manuals, IT security protocols). These exclusions likely reflect sensitivity or operational constraints and constitute a limitation on fully assessing institutional practice.

The SfSP corpus was updated in January 2025 to capture recent revisions; many universities amended these policies during 2024 to 2025, offering insight into how institutions describe early monitoring and identification of students at-risk—often via “learning” or “predictive” analytics. Rescreening for newly formalised AI policies was also conducted at that time. A comprehensive analysis of SfSPs and other related policies (for example, disability policies) would be extensive; accordingly, a high-level summary of SfSP findings is presented here.

Given the volume and diversity of materials reviewed, the analysis prioritised patterns and gaps most relevant to the themes developed in Section 7 below. The analysis does not seek to single out or name individual universities, except where naming an institution is both necessary and not unfavourable—for example, in identifying universities that have made voluntary commitments to applying the APPs, or where a policy is cited as an example of emerging good practice. University public-facing policies were the sole data sources for this analysis. Because these documents are frequently revised and updated without systematic version control or consistent metadata, URLs are particularly unreliable identifiers for this document type and are not reported in the reference list. References record the effective or approval date of the version accessed during the data collection periods described above.

6.3 Privacy policies

This subsection presents a content analysis of publicly available privacy policies sourced from all 39 Australian public universities designated as “Table A” providers as of January

2024. Institutional approaches to data and information privacy governance varied considerably in both the number of distinct policies maintained and their naming conventions. For example, some universities held more than four separate privacy-related policies in their official policy libraries, while others consolidated governance under a single framework. This is, however, consistent with guidance from the OAIC (2023a), which suggests that it may be appropriate for large institutions with complex business functions to maintain multiple, more targeted policies.

To provide a consistent basis for the analysis, a single "primary" privacy policy was identified for each university, prioritising the policy that most clearly articulated the institution's core commitments concerning the management of student personal information. This review systematically examined how these policies address five key areas:

1. their stated alignment with the *Privacy Act* (Cth)
2. the classification of data pertaining to student equity groups
3. the extent to which they recognise diverse cultural perspectives on privacy, with a specific focus on acknowledging First Nations data sovereignty principles
4. whether they acknowledge the use of personal data for advanced analytics, such as predictive analytics or ADM
5. their stipulated requirements and conditions for conducting PIAs, an indicator of institutional data privacy and governance maturity.

The findings from this examination map the current policy landscape in Australian higher education, highlighting areas where greater clarity and transparency are needed, alongside identifying examples of robust privacy governance and good practice.

6.3.1 Alignment with the *Privacy Act 1988* (Cth)

Background

As noted in Section 5, Australian universities operate within a patchwork of Commonwealth, state, and territory privacy legislation. Accordingly, only three of 39 (7.7%) Table A providers—ANU, ACU, and UNDA—are directly subject to the *Privacy Act 1988* (Cth) as a core institution-wide privacy framework. For the remaining 36 Table A providers, state or territory laws provide the primary regulatory framework, with the *Privacy Act* applying only in limited Commonwealth contexts (for example, data collected and reported under HESA via TCSI, handling tax file numbers, or performing Commonwealth contracts).

Findings

The review found that five of the 39 university privacy policies (12.8%) included an explicit voluntary commitment to applying the APPs under the *Privacy Act 1988* (Cth), though the nature and strength of that commitment varied across institutions. Notably, all five universities were located in South Australia or Western Australia—jurisdictions where, at the time of the review, state privacy legislation applicable to universities was comparatively limited. This geographic pattern suggests that voluntary alignment with federal privacy standards may provide an additional safeguard where state-level frameworks are less comprehensive.

In South Australia, public sector privacy is governed primarily through an administrative instrument—the *Information Privacy Principles (IPPs) Instruction (PC012)*—rather than a dedicated information privacy act. All three public universities nevertheless referenced the

APPs as a framework for their privacy governance (Department of the Premier and Cabinet, 2020). The nature of those commitments varied in specificity and strength: the University of South Australia adopted the APP requirements as a stated purpose of its privacy policy and applied them broadly across its personal information handling practices, though the policy does not explicitly acknowledge the voluntary nature of that commitment (University of South Australia, 2021); the University of Adelaide committed to handling personal information in a manner consistent with the *Privacy Act 1988* (Cth) and the APPs, while also explicitly recognising the *IPPs Instruction* as applicable legislation, making it the only South Australian university in this review to formally acknowledge both frameworks within its privacy policy (University of Adelaide, 2017); and Flinders University framed its commitment as best practice, explicitly acknowledging that neither the Act nor any state privacy legislation legally binds the University (Flinders University, 2023).

Western Australia shows a similar pattern. Both Murdoch University and The University of Western Australia voluntarily referenced the APPs as a governance framework, despite not being legally bound by the *Privacy Act 1988* (Cth) in most circumstances. Until recently, Western Australia had no whole-of-government privacy statute. That gap has since been addressed by the PRIS Act, which received Royal Assent on 6 December 2024 and will commence in stages. As the PRIS Act establishes a dedicated state privacy framework, universities will likely revise their privacy policies to reflect the state regime as it comes into force, while continuing to reference the APPs where relevant.

The voluntary commitments made by these five universities varied considerably in the language and rationale offered. The most explicit commitment came from Murdoch University, whose privacy policy stated:

> As a state university we are not subject to the Federal Government's *Privacy Act 1988* (Cth) however, as a commitment to safeguarding your personal information and to make you aware of how we may use it, we have initiated this *Privacy Policy* which adopts the new Australian Privacy Principles, which are set out in Schedule 1 to that Act, essentially as if we were a Commonwealth government agency. (Murdoch University, 2023, preamble)

This framing—explicitly adopting the APPs as an operational standard in the absence of a legal obligation to do so—represents the strongest voluntary commitment observed across the five universities.

The review further found that 26 of the 39 Table A providers (66.7%) acknowledged specific but limited obligations under the *Privacy Act.* Their policies typically addressed scenarios explicitly mandated by federal law, most commonly the handling of tax file numbers and data governed by HESA, including the collection of equity group indicators reported via TCSI. Policies in this group generally prioritised their respective state or territory privacy legislation as the primary governance framework, treating Commonwealth obligations as supplementary rather than comprehensive.

The review also found that four of the 39 providers (10.3%) relied almost exclusively on state or territory privacy legislation, with only limited or conditional reference to the Commonwealth *Privacy Act* or the APPs. Policies in this group did not reference HESA, which represents a notable gap given that HESA provides the key basis for the *Privacy Act's* application in university contexts, including data reported via TCSI. Most significantly, one

university privacy policy made no reference of any kind to any privacy legislation or to HESA, leaving students and staff at that institution with little basis for understanding how their personal information is governed.

Addressing fragmentation

The fragmentation of privacy regulation, from Commonwealth, state, and territory law down to institutional policy, has important practical effects. One immediate consequence is variation in the privacy collection notices (required under APP 5) presented to students when disclosing equity-related information to their university for TCSI collections. These notices shape students' understanding of how their data will be collected, used, shared, and protected, and while there is no sector-wide template—because of fragmented legislation—the Department of Education has advised providers to review their privacy notices against the 13 APPs (Department of Education, 2024b).

Emerging evidence indicates that responses to privacy collection or consent notices vary across student subgroups and are sensitive to wording and clarity. In learning analytics contexts, consent propensity correlates with factors such as institutional trust and demographics (for example, gender, race), and even small framing changes (opt-in versus opt-out) shift response rates, risking differential participation and bias in downstream datasets (Li et al., 2022). At the same time, research shows that common terms, such as "de-identified" and "confidential", are not consistently understood and that willingness to share personal information increases with perceived strength of privacy protections, with both patterns varying across demographic groups (Corman et al., 2022). These findings underscore the equity risk of heterogeneous notices across the sector and the case for clearer, more standardised APP 5 notices.

The issue of inconsistency in collection practices is not confined to notices. The Accord final report highlights persistent inconsistencies in equity data, but particularly disability, arising from divergent capture points (for example, at application, at enrolment, or during registration with support services) and varied collection practices across institutions (Department of Education, 2024a, p. 116). These concerns are further reflected in the Department of Education's (2024b) needs-based funding consultation paper. Data collection inconsistencies of this kind erode comparability, create inequalities in institutional funding for equity initiatives, and undermine the policy utility of sector-wide reporting.

In this context, greater conformity is now a policy imperative. The *Privacy Act Review Report* proposes sector-specific standardisation of templates, layouts, terminology, and icons for privacy policies and privacy collection notices, and the government has indicated in-principle agreement to this direction (Attorney-General's Department, 2022, p. 100).

Building on this, two priorities warrant attention: the development of a standardised higher education APP 5 notice template that explicitly incorporates sector-specific data reporting requirements, and the harmonisation of equity and disability definitions and capture points across the student life cycle. Both are well suited to the complementary stewardship and regulatory functions of ATEC and TEQSA, working in collaboration with the OAIC and the Department of Education.

*This section supports **R1** (life cycle guardrails) and **R3** (national baseline with shared definitions and tools).*

6.3.2 Student equity within privacy policies

Overview

Across 39 university privacy policies, most institutions mirror Commonwealth, state, and territory law by restating the statutory binary of personal information and sensitive information (which includes health information) and stopping there. In other words, privacy policies largely do not map the equity cohorts used in higher education policy (that is, disability, First Nations, low SES, regional or remote) onto explicit privacy classifications. This matters because classification drives collection thresholds (for example, informed or explicit consent), internal use and disclosure limits, and the safeguards that must apply.

Disability data (health information)

Nearly all privacy policies specify that health information is sensitive, but only 23 of 39 (59%) policies explicitly mention disability as a class of health information—largely following the language of state-level legislation—or otherwise single out disability data as sensitive in their own right. In the remainder, disability is implicitly covered via the generic health information definition. The effect is uneven signalling: while disability information will typically be handled as sensitive in practice, fewer than two-thirds of policies say so plainly.

First Nations data

Across the corpus, only one privacy policy (1/39) explicitly recognised First Nations cultural and personal information as a distinct and sensitive category—Batchelor Institute of Indigenous Tertiary Education (2016)—with specific reference to Indigenous traditions, sacred sites, and cultural sensitivities. The remaining 38 rely on the general statutory category of “racial or ethnic origin” to imply sensitivity rather than naming First Nations data explicitly. By contrast, research policy suites are more direct, with near-universal references to the *AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research* (Australian Institute of Aboriginal and Torres Strait Islander Studies [AITSIS], 2020*)*, the *CARE Principles for Indigenous Data Governance* (Global Indigenous Data Alliance, 2023), or other acknowledgements of Indigenous data sovereignty. This divergence highlights a governance gap: explicit safeguards are common in research contexts but virtually absent from privacy policies governing student administration and support.

Other equity and equity-like cohorts

For cohorts such as low SES, regional or remote origin, FiF, women in non-traditional areas, care leavers, and carers, privacy policies generally do not designate these attributes as sensitive in their own right. In practice, data about these cohorts are handled as personal information, unless they also reveal a legislatively sensitive attribute (for example, health information or racial or ethnic origin). A very small number of policies make special mentions of particular groups—for example, explicitly classing “immigration status” as sensitive (2/39) or referring briefly to “equity data” in conjunction with health information (1/39)—but these are outliers. As a result, these equity indicators are usually treated as ordinary personal information, which can overlook risks from proxies or linked data—such as postcode or service-use patterns—not captured by the statutory sensitive categories.

6.3.3 Acknowledgement of cultural differences in privacy understandings

An important dimension of privacy management, especially in diverse university communities, is recognising that conceptions of privacy and the sensitivity of both personal and group information can differ across cultural backgrounds. This is particularly significant for First Nations Australians, whose views on data frequently encompass collective rights and intergenerational significance—understandings that are not adequately addressed within current Australian legal and organisational data governance frameworks (Rana & Azeez, 2025; Rose et al., 2023; Walter et al., 2021).

The analysis of the 39 university privacy policies revealed that explicit acknowledgement of diverse cultural conceptions of privacy is exceedingly rare. Most policies focus on compliance with prevailing Australian privacy laws and their definitions of personal and sensitive information, without specific provisions or guidance encouraging staff to consider broader cultural nuances in their data-handling practices.

The Batchelor Institute's *Privacy Policy* (2016), as mentioned above, is a significant exception because it has clearly centred Indigenous perspectives within its privacy framework. Its "both-ways philosophy" explicitly "brings together Indigenous Australian traditions with western academic disciplinary contexts … including the approach to privacy", aiming for the "well-being and protection of individuals, families, clans and communities" (section 1.4). This policy demonstrates a foundational commitment to respecting and integrating Indigenous perspectives on data that extend beyond research considerations alone to also include information relating to students within the university.

La Trobe University's *Privacy Policy* contains a notable provision acknowledging that community standards in relation to privacy can be conceived differently across cultures, and that collective rather than individual conceptions of privacy may apply in some communities (2023, section 15). The policy further acknowledges that views about what constitutes personal and sensitive information "may not necessarily align with the definitions articulated under current privacy legislation" and encourages staff to be mindful of community expectations regarding privacy in addition to complying with the law (La Trobe University, 2023, section 15).

Beyond these two lone examples, the privacy policies of the remaining 37 Australian public universities appear to focus singularly on individual privacy rights as embodied in the current Australian privacy framework.

6.3.4 Personal data and advanced analytics transparency

Next, the review considered the 39 university privacy policies to see whether they make explicit the use of personal and sensitive data for learning analytics, predictive analytics, profiling, and ADM. Only a small minority do so: three of 39 directly address ADM (often with little operational detail), two mention "learning analytics", and one mentions "artificial intelligence"; there are no references to "predictive analytics", but two policies indicate the use of "profiling". While the level of detail varies, these disclosures show a gradual shift towards data-intensive digital practices (including datafication and digitalisation) aimed at improving educational and operational outcomes.

Where such uses are disclosed, the stated purposes typically centre on enhancing the student experience, supporting learning outcomes, and improving institutional services. Overall, these references mark a modest shift in how student data, often including grey data, are used: not only for administration but for more analytical and sometimes proactive purposes. Acknowledging such uses in core privacy policies is a positive step for transparency; however, inconsistent terminology, variable purpose statements, and limited detail about data sources, decision logic, safeguards (human oversight), and student options still impede clear stakeholder understanding and meaningful notice. This issue is returned to in the discussion concerning the SfSP in Section 6.4.2.

6.3.5 Privacy impact assessments

A PIA is a structured process used to evaluate how a project, system, or new initiative might affect the privacy of individuals. As a key data governance mechanism, the PIA process helps organisations identify potential privacy risks early, ideally beginning before the project is launched, and consider how to minimise or avoid any identified risks. PIAs typically involve examining what personal information will be collected, how it will be used and stored, who will have access to it, and whether its use is lawful, proportionate, and respectful of individuals' rights. In doing so, a PIA supports compliance with privacy laws while also promoting transparency, accountability, and public trust in an organisation's data handling.

It appears that only ANU is currently required, via legislation, to regularly conduct PIAs. Given that ANU is part of the Australian Public Service, it must conduct PIAs for activities that carry significant privacy risks and maintain a public register of completed PIAs under s 15 of the *Privacy (Australian Government Agencies —Governance) APP Code 2017*. This reflects ANU's unique classification as a Commonwealth agency and its responsibilities under the Australian Government's privacy framework.

PIAs are not currently required for entities subject to the *Privacy Act*; however, the *Privacy Act Review Report* (Attorney-General's Department, 2022) has recommended that they be made mandatory for activities involving high privacy risks (Proposal 13.1), to which the government has "agreed in principle". Also of importance is the clear embedding of the "fair and reasonable test" (see Section 5.2.3) within the PIA process. The review report has also recommended that guidelines be developed by the OAIC for determining when data and digital activities may be considered "high privacy risk" thereby triggering the PIA requirement (p. 124).

The analysis of 39 privacy policies revealed a mixed landscape regarding the explicit commitment to requiring PIAs. A total of 15 (38.5%) policies either mandate or strongly recommend PIAs (or similarly termed assessments) for new projects, system changes, high-risk activities, or third-party engagements. Although five (12.8%) of the policies reviewed do not explicitly mention PIAs, they imply similar processes by referencing "privacy-by-design" approaches, or general risk-based approaches. Additionally, 19 (48.7%) of the reviewed policies, approximately one-half, make no explicit reference to PIAs of any kind.

While most universities are not strictly required to conduct PIAs, state and territory legislation and regulators typically encourage the use of PIAs as a means of demonstrating that "reasonable steps" have been taken to protect personal information. In this light, explicit

commitments to conduct PIAs in a university's privacy policy suggests a proactive and voluntary adoption of best practice.

However, this landscape is evolving. For example, Western Australia's new PRIS Act is expected to introduce a more formal framework and stronger regulatory expectations about the use of PIAs by WA public sector agencies, including universities, once its provisions come into force. This development signals a shift towards more explicit and enforceable PIA requirements in some jurisdictions, moving beyond general duties or voluntary measures.

By voluntarily adopting PIAs and mandating their use via policy, universities can strengthen their privacy governance frameworks and position themselves ahead of anticipated legislative reforms. This proactive approach also enables institutions to assess equity data practices for potential privacy and ethical risks before they escalate into compliance or reputational issues.

*Section 6.2 reveals uneven privacy policy alignment, thin equity classifications, limited cultural recognition, sparse ADM disclosures, and patchy PIA practices—together motivating **R4** (above-minimum, privacy-by-design with ADM transparency and PIA thresholds), **R5** (harmonised, equity-centred policy suite with culturally safe provisions), and **R3** (ATEC or TEQSA national baselines and shared APP 5 templates).*

6.4 Students with disability policies

6.4.1 Purpose and scope

This subsection presents a synthesised analysis of Australian university (see Section 10.1) disability policy and procedure documents. University disability policies provide the clearest window into how institutions handle and disclose the sensitive information of this core equity group, both internally and externally, offering formal commitments on privacy, consent, and accountability that shape everyday practice.

For this analysis, the policies of 26 of 39 Table A providers were coded, consolidating multiple documents where relevant. Inclusion was limited to materials that (1) directly address students with disability (excluding staff-only policies, general *Disability Discrimination Act 1992* (Cth) statements or plans, and "inherent requirement" policies) and (2) described processes for the creation and distribution of Learning Access Plans (LAPs) or equivalent mechanisms (for example, Equitable Learning Plans, Reasonable or Academic Adjustment Plans).

Where multiple in-scope policies existed for a single institution, their content was combined into a single university-level record. Among the 26 included universities, most had a single student-facing disability policy or procedure (20/26, 76.9%), five had two (19.2%), and one had three (3.8%).

Thirteen in-scope Table A providers had not published a dedicated "students with disability" or "academic adjustments" policy or procedure in their public-facing policy libraries at the time of collection. These universities may instead rely on general student diversity and inclusion policies, and all universities are likely to use additional materials such as tailored privacy notices or webpages maintained by disability support units. Consequently, some student-facing information about disability-data handling may be located elsewhere (for example, targeted collection notices, online guidance, service webpages) and is not

captured here. However, the review of university privacy policies shows that the handling of disability data is rarely specified beyond general statements, leaving key operational details unclear in many cases.

Analytic focus

Disability policies were assessed through a privacy-by-design lens, including data minimisation, purpose limitation, and proactive risk mitigation, alongside considerations of transparency and student agency. Where relevant, operational constraints—including timely adjustments, staff workload, and exam logistics—were also noted. Specifically examined were external reporting transparency (Section 6.4.2), internal disclosure rules and controls (Section 6.4.3), and commitments to Universal Design for Learning (UDL) (Section 6.4.4). UDL was treated as a privacy-preserving design strategy: embedding flexibility in teaching and assessment reduces routine disclosures and bespoke adjustments, while not eliminating the need for individual reasonable adjustments.

6.4.2 External disability-data sharing transparency

Background

Universities are required to report disability-related information to government and other external bodies through multiple pathways; this review focuses on transparency statements for just two. First, under HESA and related instruments, institutions collect students' disability status (typically at enrolment or later via student systems) and report it in identifiable form to the Department of Education via TCSI (public statistical outputs are aggregated). Second, under the Disability Support Program (DSP), providers must submit de-identified or aggregate information to support funding allocations for disability services, in line with DSP guidelines and funding arrangements linked to HESA.

Analytic focus

This subsection examines whether disability policies explicitly disclose that student information may be reported to government in identifiable or de-identified forms. Other legally permitted or mandated forms of external disclosures, such as regulator notifications or court orders, are beyond the scope of this analysis.

Findings

The analysis found that transparency regarding the compulsory collection and reporting of identified student disability status via administrative data systems (TCSI or HESA) is absent from the reviewed policies. None of the reviewed policy documents mention TCSI data collections or government reporting under HESA, confirming that the administrative reporting function remains structurally separated from public-facing disability policies.

This does not mean students receive no notification at all. Data collection notices and enrolment documentation may disclose government reporting obligations at the point of collection. However, such notices are transactional and do not substitute for a standing, publicly accessible disclosure in a central policy document. University privacy policies offer little additional clarity: as Section 6.3 found, most make only vague reference to the *Privacy Act* or HESA obligations without specifying what is reported, to whom, and in what form. A student seeking this information would find it difficult to locate and piece together.

This consistent absence across the corpus points to an important structural observation: these policies are developed and maintained primarily by student support units and appear

to be organised around the Disability Standards for Education's mandate for internal service delivery and consultation. This leads them to emphasise the careful handling of, and consent processes for, internal disclosures and staff permissions, while structurally excluding information that falls outside the operational remit of those units, such as administrative reporting via TCSI.

Only two of the 26 policies reviewed (7.7%) provided specific transparency about the de-identified, aggregate reporting required for DSP funding acquittals. This pattern confirms that disability policies serve primarily internal operational purposes rather than comprehensive external disclosure. Combined with the limited detail on disability data handling practices found in the university privacy policies examined earlier, a significant transparency gap remains for students seeking to understand how their disability information is collected, used, and reported.

6.4.3 Internal disability-data privacy practices

Background

This subsection examines university disability policies for indicators of privacy management across two central features of internal data practice: how institutions structure the internal disclosure and distribution of LAPs, and whether policy text explicitly states that LAP content is limited to adjustment details, excluding medical diagnoses.

Internal LAP disclosure model

The *Disability Standards for Education 2005* (Cth) require providers to consult with students, implement reasonable adjustments in a timely manner, and protect confidentiality. In practice, these obligations can create a number of important design trade-offs between student agency and operational reliability. Each of the 26 in-scope universities was classified into one of three disclosure models, or designated as unclarified where public-facing policy or procedure is silent on the operational detail (see Table 1):

1. Student distributed – Students choose who receives their LAP and when, but are responsible for distribution.
2. Service distributed (with granular consent) – The disability service coordinates sharing on the basis of explicit student permissions.
3. Blanket distribution (role-based) – Authorised staff automatically receive relevant LAP data under prior, general student consent.

Where public-facing policy and procedure do not provide sufficient operational detail to classify the model, the institution is designated as unclarified.

Table 1: Internal LAP disclosure model—benefit and risk comparison

Model	Student agency/burden	Reliability/ timeliness	Institutional burden
Student distributed	High agency / High burden	Low–Moderate	High
Service distributed (with granular consent)	Moderate agency / Moderate burden	Moderate	Moderate
Blanket distribution (role-based distribution)	Low agency / Low burden	High	Low

Findings

Across the 26 universities, the primary model for internal disclosure breaks down as follows: unclarified in 11 of 26 (42%), student distributed in seven of 26 (27%), service distributed in six of 26 (23%), and blanket distribution in two of 26 (8%). Nearly half of the policies do not state who actually shares the plan or notification with staff, remaining at the level of principles and privacy commitments rather than operational steps. Where policies do specify a mechanism, student handover is the most common default, with a comparable cohort adopting service-distributed sharing under explicit consent controls; fully automated and blanket, role-based distribution is uncommon.

A consistent pattern across institutions is the distinction between notifications intended to inform course or unit coordinators and those targeted towards examinations: even where LAPs are student distributed, exam arrangements are frequently centrally coordinated, producing layered models in practice. Service-distributed models typically emphasise written or express consent and need-to-know minimisation, while the few blanket distribution or role-based models usually retain opt-out or consent qualifiers.

The prevalence of unclarified policies represents a meaningful gap in transparency and accountability. Students and staff cannot rely on predictable, auditable processes where the operational pathway—who sends what, to whom, and on what consent basis—is not publicly stated. There are clear opportunities for institutions in this group to make these processes explicit across both teaching and examination contexts.

LAP information minimisation

The analysis next examined whether university disability policies and procedures explicitly state that LAPs, or their equivalents, record only the information necessary to implement reasonable adjustments and exclude diagnoses or detailed medical information. Each institution was coded according to the presence or absence of explicit content-minimisation language, such as “functional impact only”, “no diagnosis”, or “purpose-limited disclosure”.

Findings

Explicit LAP content limits are uncommon across the 26 universities reviewed. Only one of 26 (3.8%) includes a clear “no diagnosis” clause, explicitly prohibiting inclusion of the nature of the disability in the plan. A further three of 26 (11.5%) include explicit minimisation or purpose-limited language, such as “functional impact only”, “minimum necessary”, or “solely for implementing reasonable adjustments”. The largest group, 15 of 26 (57.7%), implies minimisation by describing plans as documenting supports, adjustments, or functional

impacts, without explicitly excluding diagnosis. The remainder, seven of 26 (27%), are silent or unclear at the plan level and rely on generic privacy language rather than LAP-specific content rules.

Where explicit clauses do appear, they are most often located in procedures rather than high-level policies and typically pair purpose-limited disclosure with an explicit exclusion of diagnosis or medical detail. Overall, the pattern reflects a broadly shared intent towards data minimisation but uneven specificity in how that intent is articulated: practice norms are widely understood among disability support units, yet they are not consistently stated in policy. To improve consistency and accountability, policies should include brief, clear clauses specifying that plans record functional impacts only, exclude diagnostic information, and are shared only for the purpose of implementing adjustments—so that students and staff can rely on consistent and predictable rules.

These policy commitments should also be reflected in the digital tools and workflows used to distribute LAPs. Where universities are selecting or configuring systems to support this process, a privacy-first approach would ensure that plans are shared only with the staff who need them, contain only the information necessary to implement adjustments, and are managed with clear student consent and time-limited access. Designing these systems thoughtfully offers a practical opportunity to embed good privacy practice into everyday operations, rather than leaving it to individual judgement.

6.4.4 Universal Design for Learning as privacy-by-design

Background

In this subsection, UDL is treated as a privacy-preserving approach to learning design that, consistent with privacy-by-design, addresses disclosure risks upstream as a design problem. By embedding flexibility and multiple means of engagement, representation, and expression into the default design of teaching and assessment, UDL reduces routine needs for individual disclosure and the circulation of LAPs for common adjustments such as time flexibility and alternative formats. This operates in a manner analogous to data minimisation and privacy by default; fewer accommodation requests mean fewer instances where disability status or sensitive details must be shared with university staff. Importantly, UDL does not replace legal entitlements to individualised reasonable adjustments for atypical or intensive needs (see Whitwell & Clarke, 2023, for an explicit treatment of inclusive pedagogy as privacy protective).

While CAST's UDL Guidelines 3.0 (CAST, 2024) do not address data privacy or disability disclosure directly, Consideration 7.4 recommends that educators vary both the requirements for public display and evaluation, and the social demands required for learning or performance. This has a direct bearing on the conditions under which students may feel compelled to disclose a disability. Related considerations, such as optimising learner choice and autonomy (7.1) and addressing biases in modes of expression and communication (5.4), further support environments where students need not expose personal information to access appropriate learning conditions. Together, these considerations reflect a learner-centred design orientation in which designing for learner differences from the outset reduces the conditions that make disability disclosure necessary.

Findings

The review of 26 university disability policies found that 13 of 26 (50%) make no policy-level commitment to UDL or universal or inclusive design. Five of 26 (19.2%) make strong, explicit commitments, and a further eight of 26 (30.8%) reference universal or inclusive design in general terms without setting clear expectations. In practical terms, fewer than half of the universities set an expectation that curricula and assessment will be designed for variability by default, and explicit UDL language is uncommon in disability policies specifically. It is worth noting that UDL commitments may be more prevalent in teaching and learning or assessment procedures than in disability policies—the scope of this review may therefore undercount the extent of UDL adoption across the sector.

Effective implementation in course and assessment design is essential to realising the privacy benefits of UDL. The framework does not remove the need for individual adjustments in all circumstances. Where LAPs or equivalent instruments are in use, consent and need-to-know principles continue to apply. The primary privacy contribution of UDL is therefore not the elimination of individual accommodation, but a reduction in the volume and sensitivity of information that must routinely circulate—lowering systemic disclosure risk across the learning environment as a whole.

*Section 6.4 identifies gaps in external transparency (HESA/TCSI, DSP), uneven internal disclosure models and minimisation rules for LAPs, and limited policy-level UDL commitments, together motivating **R4** (privacy-by-design in services and systems), **R5** (harmonised disability or privacy policies with explicit minimisation and notice language), **R8** (executive resourcing and clear decision rights for frontline practice), and **R7** (structured engagement with lived-experience and First Nations expertise).*

6.5 Data governance policies

6.5.1 The role and purpose of data governance policies

Background

While both privacy policies and data governance policies are essential for the responsible management of information within universities, they serve distinct purposes and target different audiences. Privacy policies are primarily externally facing documents intended to provide transparency to individuals, including students, staff, and the public, about how their personal information is collected, used, disclosed, and managed. Mandated under Australian privacy law, privacy policies must explain individuals' rights and the institution's obligations regarding personal data.

In contrast, data governance policies, or information management policies, are largely internally focused frameworks. Their primary audience is university staff and those with specific data-related responsibilities, and their main objective is to establish the internal rules, roles, responsibilities, and processes for managing the university's data and information assets effectively and strategically. As Khatri and Brown (2010) put it, governance is about "what decisions must be made … and who makes the decisions" regarding data assets, aiming to ensure data quality, integrity, security, compliance, and the use of data as a strategic asset (p. 148). Thus, these policies are geared towards internal

control, compliance, and optimising data value, rather than direct public transparency about individual data rights.

Sector frameworks—for example, the UK Jisc Data Maturity Framework (2024)—characterise comprehensive data governance as treating data as an institutional asset, establishing clear accountability from the vice-chancellor down, naming information owners or managers, and underpinning practice with policies, standards, and mechanisms for assurance, risk, and stakeholder engagement. While Australia currently lacks a sector-wide, university-specific data governance framework, institutions can adapt such models to local regulatory settings (for example, *Privacy Act 1988* [Cth], TEQSA) and their internal accountability structures.

Analytic focus

Of the 39 universities in the study, 27 (69%) met the threshold for inclusion in this analysis. Data governance frameworks vary considerably in how they are structured and named across the sector. Some universities maintain a single comprehensive policy, while others distribute equivalent content across several documents. For this reason, inclusion criteria were applied at the institutional rather than individual policy level. To be included, an institution required at least one policy document that both established a data-risk classification system and clearly assigned data governance decision-making and accountability responsibilities to defined roles. The 27 in-scope institutions contributed a total of 34 policy documents to the analysis corpus, with most institutions represented by one or two documents. It is worth noting that some of these documents use “information” or “privacy” rather than “data governance” in their titles, reflecting the absence of a uniform naming convention across the sector.

The 12 excluded universities indicate that data governance policy has not yet reached full saturation across the sector. Several had only data classification or security policies lacking clear decision-making and accountability structures, and at least one university had a vice-chancellor-level committee whose terms of reference signalled that a data governance framework was still in development.

Data governance models

Khatri and Brown (2010) defined data governance as determining “who holds the decision rights and is held accountable for an organization's decision-making about its data assets” (p. 149), and conceptualised the locus of accountability for each decision domain as existing along a continuum between centralised and decentralised models (p. 151). This review borrows that framework to examine how the policies analysed here establish decision-making authority and accountability.

Following this pattern, the review classified models as “centralised” when decision rights and standards are explicitly vested in enterprise roles or committees (for example, chief information officer, chief digital officer, information governance board), with mandatory language (“must” or “shall”) and evidence of enforcement (approvals, monitoring, exception control). “Hybrid” was used where enterprise data handling standards are detailed but day-to-day choices are delegated to faculties or divisions within defined guardrails. “Decentralised” would require clear local autonomy with minimal enterprise gatekeeping (none met this bar). Policy documents that lack sufficient detail to decide were marked “not determinable” to avoid overinterpretation.

Findings

Of the 27 universities reviewed, 13 (48%) were classified as centralised, eight (30%) as hybrid, six (22%) as not determinable, and none as decentralised. The absence of decentralised models in the sample is likely a function of the corpus itself: institutions without a formal data governance policy were not captured by this review, yet the absence of such a policy is itself a plausible indicator of a decentralised and heavily localised governance model operating by default. The findings therefore probably undercount less formalised governance arrangements across the sector.

Across centralised and hybrid policies, a common governance architecture emerges. Enterprise authority for principles, policy settings, and strategic direction is typically vested in senior roles such as a chief information officer, chief digital officer, or an information governance committee or board, while operational responsibilities are delegated to domain roles—variously termed data or information custodians or stewards—who manage day-to-day decisions within their areas.

The scope of these policies also varies. Many explicitly exclude research data, which are often governed under separate frameworks, while others are narrowly focused on “critical data,” typically data deemed essential to university operations. This suggests that governance intensity is not applied uniformly across all institutional data, potentially leaving a significant volume of grey data—data that are neither classified as research nor deemed critical—effectively ungoverned (Borgman, 2018).

6.5.2 Is equity centred in data governance policy?

Background

Data security and risk classification systems are a core feature of institutional data governance. Such systems categorise data assets by sensitivity, criticality, and the potential impact of unauthorised disclosure, modification, or loss, linking each category to handling rules governing access, storage, transmission, and retention. Classification schemes in the policies reviewed typically comprise three to five tiers. Responsibility for applying classifications is commonly delegated to domain roles such as data stewards, custodians, or information owners. The *Privacy Act* establishes baseline categories of personal information and sensitive information, but these legal categories do not automatically translate into operational handling rules. Student equity data presents a particular challenge in this respect. Data such as disability status, First Nations identity, care experience, or socio-economic background may qualify as sensitive information under the Act, while equity-adjacent proxies such as postcode or support service-use patterns may not, yet both can carry significant re-identification risk in institutional contexts.

Analytic focus

This section asks whether data governance policies go beyond *Privacy Act* classifications to explicitly centre equity data by further clarifying its status within their risk and classification frameworks, and whether that recognition, where it exists, translates into concrete handling rules. As in the analysis of privacy policies in Section 6.3.2, an equity-focused lens is here applied to university data governance policies.

Findings

A small minority of university data governance policies (four of 27) explicitly place equity data, or certain forms of equity data, in an elevated sensitivity category and tie that recognition to stronger handling rules. Federation University's *Information Technology Services Operations Manual* (2024) classifies “identifiable equity and minority group data” as “protected”, its highest risk tier, alongside health information and personally identifiable information, linking the classification to concrete access, storage, and transmission controls. UNDA’s *Information Management (Procedure)* (2024) defines “equity information” as a named category, encompassing disability, Aboriginal and Torres Strait Islander status, low SES, regional or remote background, NESB, and FiF status, and notes that this category was added as an example of “highly sensitive” data in the 2024 update (see Section 13.4.2 and version notes). ANU's *Information and Data Classification (Standard)* (2022) similarly lists “identifiable equity and disability data” as an explicit example within its highly sensitive tier, placing it alongside medical, legal, and financial information.

ANU is also notable for a second and distinct provision. Its *Data Governance (Policy)* (2022) includes a commitment to “inclusive, open and respectful governance of personal and Indigenous data” as an enterprise-wide principle. The University of Queensland's *Data Handling Procedure* (2024) goes further, requiring that the handling of Indigenous data align with the AIATSIS Code of Ethics, and specifying that the Code's principles apply beyond research to any activities that can impact or be of importance to Aboriginal and Torres Strait Islander peoples. Both provisions are significant because, in contrast to the privacy policies reviewed in Section 6.3.2, Indigenous data governance principles are not confined to the research domain alone.

Discussion

In most policies, equity data governance is indirect. Safeguards flow from general rules for personal or sensitive information, meaning equity attributes and proxies only inherit protections when the link to an identifiable individual is straightforward. Data that could identify someone indirectly, through small group sizes, combined attributes, or analytical outputs, may receive no additional protection at all, leaving contextual risks involving equity data in a governance grey zone.

The stronger exemplars in the corpus do three things well. First, they name equity categories explicitly and place them at higher classification tiers. Second, they link those tiers to operational controls covering access approval, storage and transmission, data use limitations, and retention and disposal. Third, and most rarely, they specify how derived artefacts such as learning analytics outputs or risk scores either inherit higher risk classifications or trigger reassessment under stricter controls. Where these elements are absent, the handling expectations for equity data remain in a governance grey zone across domains, leaving staff without clear guidance and students without the protections those policies should provide.

Summary

Implementation of data governance policies is uneven: roughly two-thirds of universities publish a dedicated governance instrument, models are largely enterprise-led with centralised implementation and variable decision rights, and multi-tiered data-risk classification is common but inconsistently operationalised, leaving pockets of grey data that

fall outside both dedicated research data governance regimes and the broader institutional data frameworks.

Two specific gaps were also observed. Evidence of student voice or participation in data governance mechanisms is effectively absent: 26 of the 27 policies reviewed contained no such mechanism, and the remaining policy offered a values-level commitment only. Similarly, no explicit governance of student data used for program evaluation was found. No university data governance framework reviewed set conditions distinct from course evaluations or research, and where evaluation occurs, oversight appears inferred from generic privacy or security controls rather than formally set out in policy.

*Equity is rarely explicit in data governance settings. These gaps motivate **R5** (harmonise and centre equity across the policy suite), **R4** (above-minimum, privacy-by-design controls with role-based access, retention, and model-risk management), **R7** (structured participation in governance bodies), and, for evaluation activities**, R6** (a defined oversight pathway).*

6.5.3 Support for Students Policies: Where data and digital meet

Background

Traditionally, universities have typically addressed student failure through “academic progression monitoring,” a reactive regime triggered after poor results (for example, failed units, low grade point average) and based almost exclusively on summative outcomes. By design, these processes engage supports only once a student has already demonstrated unsatisfactory progression.

By mandating in-semester, unit-level identification of at-risk students, the SfSP, in effect from 1 January 2024, moves intervention earlier and necessitates close to real-time analysis of far more refined student data than final grades alone. In practice, many universities now draw on the grey data generated by learning and administrative activity (for example, LMS engagement, attendance and submission patterns, early assessment signals, advising or administrative flags), often analysed via learning analytics and predictive methods. SfSPs therefore provide a valuable test case for proactive risk monitoring, analytics-enabled student support, and how universities explain these data-driven practices to students in formal policy. Because at-risk monitoring depends on both the data collected and the systems that analyse or act on them, SfSPs sit at the junction of data governance and digital governance.

Analytic focus

This subsection examines 38 of the 39 SfSPs in the corpus; one policy was not publicly available at the time of review. The review looked both at practice, including workflows, triage, outreach, and referral, and at transparency, including purpose, data use, and student agency. Specifically, it asked whether policies make clear how academic risk is identified at the unit level and what personal data are used to do so. Policies were then classified by the clarity and specificity with which they describe these analytic methods and data inputs.

How SfSPs were grouped

Each policy was coded on four dimensions: (i) timing clarity: does it specify proactive, in-semester, unit-level monitoring rather than end-of-term (reactive) checks? (ii) data-source clarity: are the source systems or data types used for risk signals identified? (iii) analytic-

method specificity: are indicators, techniques, or approaches named (for example, LMS engagement, early assessment, “analytics”, “modelling”, “propensity”)? and (iv) linkage to governance: does it point to relevant learning analytics, AI, data, or privacy instruments?

The primary split is whether the SfSP confirms proactive, in-semester monitoring (Group B) or is too general to establish this (Group A). Within Group B, the review distinguished B1 (Detailed: indicators, systems, techniques named) from B2 (Generic: early monitoring stated, but methods described only broadly). Because it cuts across both groups, transparency about equity or sensitive variables as model inputs is treated separately.

Group A – General and Opaque SfSPs (11/38; 29%).
Policies in this group state that the university identifies or supports at-risk students but do not specify the timing, data sources, or analytic methods for early, unit-level monitoring. Procedural detail is often pushed to generic academic progress or monitoring instruments that themselves lack in-semester measures; links to analytics or privacy governance are typically weak or absent. The result is limited operational transparency within the SfSP.

Group B – Proactive and Specified SfSPs (27/38; 71%).
These policies confirm proactive, in-semester monitoring and were divided into two subgroups:

- B1 – Detailed (*n* = 19). Policies name early-warning indicators (most commonly LMS engagement and early assessment performance), identify source systems, and in some cases explicitly refer to “analytics”, “predictive modelling”, or related techniques.
- B2 – Generic (*n* = 8). Policies make clear that early monitoring occurs but describe how it is done only in broad terms within the SfSP.

Across Group B, explicit references to equity or sensitive characteristics as input variables in early-risk models are uncommon, and the terminology employed (for example, “engagement monitoring”, “data-informed”, “analytics”) is often imprecise. Some SfSPs link to learning analytics or AI governance documents, but consistency is low.

Focused analysis: Universities indicating use of advanced analytic techniques

Ten institutions, all in Group B and mostly in the B1 (Detailed) subcategory, explicitly mention or clearly describe the use of advanced analytics in their SfSPs. References commonly include “learning analytics”, “predictive modelling”, “predictive analytics”, or “propensity”, cited directly in the policy. The depth of explanation varies: most SfSPs name the technique and purpose, for example early identification and targeted outreach, but do not detail inputs, model logic, thresholds, validation, error rates, or human review. A review of associated data governance, privacy, AI, and learning analytics instruments, where available, showed that several universities have or are developing more robust governance frameworks, for example dedicated AI or learning analytics policies. However, cross-referencing from the SfSP to these governance documents is inconsistent, leaving lines of accountability and oversight unclear within the SfSP itself.

The transparency challenge

A cross-cutting finding, even among the 10 analytics-explicit SfSPs, is limited transparency about whether and how student equity characteristics or other sensitive data are used as inputs in early-risk models. Many universities signal tailored support for equity cohorts, yet it

is rarely clear whether those characteristics are factored into predictive models that flag students as at-risk. Only two SfSPs explicitly state that equity categories or groups are included as key factors or indicators and that these cohorts are prioritised for intervention.

Even in these cases, crucial details remain unspecified: which attributes are used, how they are encoded or weighted, which systems supply them, whether their role is a model input or a post-model triage rule, and what safeguards, for example human oversight, bias testing, and appeal routes, are in place. As a result, students and staff have no clear basis for understanding how equity-related data are used to identify, support, or sort them.

Example of emerging good practice: The University of Wollongong

With limited research in this area, it remains premature to prescribe “good practice”. There is no settled view of what ideal, or even adequate, practice looks like for equity students and the handling of personal or sensitive information in the Australian context. Key questions persist: How much information is sufficient? When or how should it be communicated? How many policies are needed, of what type, and for which audiences? What language best supports clarity across diverse stakeholders? Even so, it is useful to highlight emerging examples while the sector begins to engage more systematically with these challenges.

Among several promising cases, the University of Wollongong (UOW) offers a policy framework that seeks to address the grey areas of equity work as data work. UOW's SfSP (University of Wollongong Australia, 2023a) stands out for its effort to explain how the university conducts early, in-semester at-risk monitoring and how equity characteristics or groups are considered in that process. Importantly, the SfSP includes an in-text link to the *Learning Analytics Data Use Policy* (University of Wollongong Australia, 2023b), which elaborates analytic processes, privacy safeguards, and measures to minimise adverse impacts.

UOW's broader framework references tools and mechanisms that directly address equity-related risks. These include internal instruments not available for public review—namely, *Guidelines for Actioning Learning Analytics Insights* and a *Procedure for Monitoring Comparative Student Outcomes*—as well as the publicly available Jisc (UK) Code of practice for learning analytics (Jisc, 2015). UOW’s SfSP also references and links to a *Data Governance Procedure*, *Privacy Policy*, and *Data Handling Guidelines*, though not all these documents are publicly accessible.

Data access governance is also well articulated: the learning analytics data warehouse requires approval from the Deputy Vice-Chancellor and Vice-President (Academic and Student Life), even for “business as usual” recipients, and a Learning Analytics Advisory Group provides program-level oversight. Together, these instruments begin to connect policy intent, namely student support and fairness, with operational controls covering access, approvals, and cross-referenced guidance. This is precisely the junction where many institutions' frameworks are currently thin.

Discussion

Without claiming UOW as a definitive model, three features of its framework are especially instructive for the sector. First, the UOW SfSP provides a plain-language explanation of how early monitoring works and where equity considerations arise. Second, live cross-references connect the SfSP to learning analytics and data governance policies that spell out methods and safeguards. Third, clear access and oversight structures, including named approvers, an

advisory group, and internal guidance, make the framework more auditable as practice evolves. Together these elements improve intelligibility for students and staff and offer a practical starting point for institutions seeking to strengthen their own frameworks.

The UOW example is a useful starting point for universities still building data, digital, and equity-related policy frameworks, but it also surfaces broader sector issues. Is “learning analytics” still the right umbrella for practices that now include predictive modelling and, increasingly, AI? If not, how should AI governance intersect with, or encompass, these activities referenced in many SfSPs? UOW's statement that students cannot opt out of learning analytics on duty of care grounds spotlights unresolved questions about student autonomy and heightened privacy needs for particular cohorts.

Three priorities warrant sector-wide attention. First, terminology and policy architecture: what these practices are called and where they sit, whether in SfSPs, learning analytics, AI, or data governance instruments, with clear cross-references between them. Second, lawful and ethical basis and baseline mitigations: when consent or opt-out is appropriate, and what minimum safeguards apply if it is not, for example transparency, bias testing, human oversight, and appeals. Third, equity safeguards: how equity and sensitive attributes are used as model inputs or post-model triage rules, and how their use is documented, monitored for impact, and overseen.

*Section 6.5.3 finds that while emerging exemplars such as UOW demonstrate how policy intent and operational controls can be connected, most SfSPs lack transparency about analytic methods, equity data inputs, and oversight structures, motivating **R4** (above-minimum, privacy-by-design implementation with ADM transparency), **R5** (harmonised treatment across the policy suite), **R6** (a defined, proportionate oversight pathway), and **R7** (student and staff participation).*

6.5.4 Policy fragmentation and the transparency challenge

Despite genuine effort across the sector, fragmentation continues to shape how student equity data are governed and understood. At many institutions, policy instruments for privacy, data governance, learning analytics or AI, and support for students sit in separate silos, use inconsistent scope and terminology, and are weakly cross-referenced. As a result, students, staff, and even internal decision-makers struggle to see how equity-related data are collected, combined, and used to flag risk, who is authorised to access or share it, and what safeguards, including minimisation, need-to-know, retention, audit, and appeal, actually apply.

In practice, key operational details, including data flows, decision rights, role-based access, model inputs and thresholds, and oversight and review, are often dispersed across multiple documents or omitted altogether, producing uneven implementation and avoidable gaps in trust and accountability. A clearer policy architecture that links these elements end to end, supported by defined oversight pathways, participatory governance, and adequately resourced frontline practice, is precisely what R3 (national baseline with shared definitions and tools), R4 (above-minimum, privacy-by-design implementation), R5 (harmonised treatment across the policy suite), R6 (a defined, proportionate oversight pathway), R7 (student and staff participation), and R8 (leaders to model and resource privacy by default) are designed to support.

7. Qualitative study: Centring the views and experiences of equity practitioners

7.1 Overview

Section 5 of this report outlined the macro-level legislative and regulatory context governing the use of data and digital technologies in Australian universities. Section 6 provided an overview of the meso-level landscape, examining institutional policies, procedures, governance structures, and transparency mechanisms. Across the macro and meso levels, increasing layers of governance fragmentation and complexity were observed, revealing the many sources of the grey and murky landscape that equity practitioners, and students, must navigate. In Section 7, the focus shifts to the micro level, exploring the experiences and perspectives of university staff engaged in equity and data work on the ground. Foster et al. (2018) argued that structural conditions at the macro and meso levels significantly shape this micro level by influencing how data work—and consequently their associated production of both value and risks—is experienced by individuals working within their specific institutional contexts.

According to Foster et al. (2018), various professional groups contribute both directly and indirectly to shaping the micro context of "data work" within institutions. They identified three primary categories of professionals: first, those directly involved in extracting value from data through tasks such as data wrangling, analysis, reporting, and visualisation; second, end users who rely on provided data to inform their decisions and actions, or who generate their own data to fulfil their professional responsibilities; and third, individuals with supervisory and strategic roles, ensuring effective governance, appropriate data usage, and data security.

In practice, particularly within student equity work, these roles often overlap and are rarely clearly delineated, yet each remains essential to comprehensive data work. Foster et al. (2018) emphasised that this micro level constitutes the lived professional environment, where the balance between the value and risks associated with data work is actively negotiated among diverse professional groups and institutional stakeholders.

Section 7 of this report presents the core contribution of this Fellowship research project. This qualitative study explored the perspectives and experiences of student equity practitioners, senior university leaders, and staff in data analysis roles as they navigate the intersection of equity work and data work within the micro-level context of institutional practice. A key objective of the Fellowship was to amplify the voices of equity practitioners, whose roles are critical in both realising the potential benefits and managing the inherent risks of student equity data work.

This research addresses a significant gap in the existing literature by offering important insights into the perspectives and experiences of university equity practitioners, senior leaders, and data analysts who are substantially involved in student equity and data work. These areas are largely underexplored in the Australian context, and this study contributes

new evidence to an important gap in the Australian research literature. In the Australian research literature, student views on privacy and learning analytics have been a clear focus of research (Soffer & Cohen, 2024). There have also been several studies capturing the views of Australian university staff on the governance and use of student data. For example, Braunack-Mayer et al. (2023) interviewed Australian higher education "researchers and teaching specialists in learning analytics and/or data analytics" (p. 3). These studies have identified widespread concerns about privacy, transparency, and consent, and further raised concerns about the oversurveillance of "already-vulnerable or stigmatised groups (including First Nations peoples and students with mental health problems …)" (Braunack-Mayer et al., 2023, p. 9).

Despite the growing body of literature on student and staff perspectives regarding data and digital governance in Australian higher education, research focused specifically on the views of student equity practitioners remains extremely limited. This absence is notable, given that those working most closely with equity cohorts bring distinct, practice-informed insights into the effectiveness of data governance at the micro level, where equity work and data work intersect. Addressing this gap was a central aim of the present study. While Braunack-Mayer et al. (2020) noted a general lack of stakeholder engagement in policy development, it appears that equity-focused staff are among those missing voices.

7.2 Methods

7.2.1 Ethics approval

Ethics approval for the project was provided by La Trobe University's HREC [HEC24361].

7.2.2 Approach

Because this is a largely uncharted area of research, the study employed an exploratory qualitative design grounded in a naturalistic research paradigm. Naturalistic inquiry prioritises studying phenomena in real-world settings, enabling researchers to grasp experiences and views of participants in an in-depth and contextualised manner (Lincoln & Guba, 1985). This paradigm is particularly apt for complex topics with little prior investigation, offering a flexible yet systematic framework for capturing and analysing nuanced human experiences as they unfold in authentic contexts (Creswell & Poth, 2024). Accordingly, this methodological choice allowed the project to examine, in a comprehensive manner, how equity practitioners and other university staff perceive current challenges and identify opportunities for stronger data and digital governance.

The earlier research stages exploring RQ1 and RQ2 were useful in informing the subsequent aim of the Fellowship's third research question:

> **(RQ3):** What challenges and opportunities do student equity practitioners and senior university leaders identify in balancing the value and risks of student equity data within current governance frameworks and cultures?

This high-level research question was further refined into three specific aims guiding the qualitative component of this Fellowship. The research sought to explore the confidential views of student equity practitioners and university leaders in relation to:

1. the approach to data and digital governance that their institutions have adopted
2. the challenges they have encountered in collecting, controlling, and using equity student data to support student success
3. the opportunities they see for improving the governance and responsible use of student equity data.

7.2.3 Participant selection

Participants for this research were recruited via purposive sampling and according to the following selection criteria:

- they are a current staff member of an Australian public university, and
- their role may be described as a student equity practitioner—or someone significantly involved in providing support services to undergraduate students identified with an “equity group”, or
- their role is significantly related to the senior leadership or management of student equity strategy or support services, or
- their role is significantly related to the analysis, management, or governance of student data and digital technologies.

The participant selection criteria ensured relevance and depth, supporting the study’s objectives by capturing diverse yet comparable perspectives across the sector. These three target participant groups are also closely aligned with the three professional groups identified by Foster et al. (2018) as being most significant to influencing the micro context of “data work” within institutions.

7.2.4 Participant and institutional diversity

Maximum-variation sampling (Creswell & Poth, 2024) was employed to ensure diversity and relevance across institutional types, geographic regions, and professional roles and levels of seniority. The final participant sample comprised 21 participants (nine males and 12 females) that collectively achieved the desired diversity along each of the relevant dimensions. The strict privacy protocols and research ethics commitments of this research do not allow participant institutions to be identified; therefore, only a high-level aggregate summary of participant characteristics is provided here.

To ensure a spread of institutional perspectives, four broad tiers of seniority were identified, and participants were purposively recruited from each level. The final sample of 21 participants included five executives, five directors, five managers, and six professionals.

The study did not separate staff into “academic”, “professional”, or “general” categories because these labels are largely arbitrary, reflecting only a person’s current classification and revealing little about the diverse work they perform in practice. It is also notable that three participants are in roles with a data and analytics focus. Furthermore, five participants indicated that they hold senior data governance roles described as a data or information steward, owner, or custodian within their institutions.

To capture a diverse range of roles, the purposive sampling also considered each participant's specific responsibilities. Although all participants are engaged in equity work and data work, a particular effort was made to include staff who work with equity groups recognised as requiring greater sensitivity under Australian privacy and anti-discrimination law—namely, First Nations students and students with disability. Overall, five participants have direct responsibility for supporting First Nations students, and 10 for supporting students with disability.

To be clear, while well over half of the participant pool work directly with these more sensitive cohorts, all participants in this research would carry responsibilities to work with students belonging to these cohorts or with their data.

Institutional diversity was also monitored and targeted throughout the recruitment process. The final sample contains participants drawn from 12 universities located in six Australian states and territories. These institutions are also drawn from each of the major Australian university representative groups—Group of Eight, Regional Universities Network, Innovative Research Universities, Australian Technology Network—as well as independent universities. Regional universities and universities with regional campuses were also well represented in the sample.

7.2.5 Data collection

Semi-structured interviews were conducted remotely on Microsoft Teams and recorded in both audio and video format. Participants received an interview guide (see Appendix Section 10.2) with nine illustrative questions ahead of their session. Given the variation in institutional context, seniority, and role, the guide served as a flexible prompt rather than a checklist; not every question was expected to be covered. In keeping with the study's exploratory, naturalistic design, each conversation was allowed to evolve, foregrounding the interviewee's own experience, institutional knowledge, and particular interests or concerns.

The average interview length was 62 minutes. Interview topics included institutional data and digital governance practices, perceived barriers and challenges in ethical data collection and handling, and participant insights regarding potential governance improvements.

7.2.6 Data management

Data management adheres to strict ethical guidelines, employing secure digital storage provided by La Trobe University digital research services. Audio and video recordings and preliminary transcripts were securely maintained, with transcripts undergoing de-identification and editing by the principal investigator (the Fellow).

Participants were invited to review, edit, and ultimately approve their respective transcripts to ensure accuracy, authenticity, and appropriate personal and institutional de-identification. Once transcripts were approved by the participant, the original recordings were securely deleted. All transcripts were anonymised, systematically removing identifying institutional information, retaining only generalised role descriptions (for example, practitioner, manager, director, executive). This comprehensive approach to data collection and management ensured participant confidentiality, supported ethical integrity of the project, and contributed to assuring the validity of the data collected.

7.2.7 Data analysis

Each interview was transcribed and edited for anonymity shortly after completion. Final transcripts were analysed using reflexive thematic analysis, following Braun and Clarke's (2019, 2021) six-phase process. Initial coding and theme development were undertaken in NVivo 15, with the Fellow manually coding each transcript on a line-by-line basis. This approach emphasised close engagement with the data and allowed for inductive theme generation, while remaining attentive to the broader policy and practice context in which participants' experiences were situated. Throughout the process, reflexivity was maintained by documenting analytic decisions and iteratively refining themes considering both the data and the research aims.

7.2.8 Limitations and transferability

As with any qualitative study, this research has several limitations that should be clearly acknowledged. First, the findings are based on the views and experiences of participants working within particular institutional and policy contexts. As described in Section 5, Australian universities operate under different macro-level laws and regulations depending on state and territory jurisdiction. Some important meso-level institutional policy differences must also be kept in mind, and these were described in Section 6 of this report.

More importantly, the experiences and views shared by each participant in this research are shaped by their professional context, background, training, and relative position within their institution. Therefore, the perspectives presented here are necessarily subjective and should not be assumed to represent all practitioners or institutions. Care has been taken to ensure that claims grounded in interview data are supported, where possible, by documentary analysis, publicly available policies, or relevant scholarly literature. This triangulation increases the trustworthiness of the findings and suggests that many of the issues raised are likely to be transferable across institutions—particularly within the Australian higher education context.

Finally, while every effort has been made to present insights with fidelity to participants' intent, ethical considerations, particularly the need to preserve anonymity, mean that specific individuals, institutions, or systems referenced in interviews are not identified. Where relevant practices or strategies are publicly documented, or common across institutions, these have been cited to support further exploration and adaptation by institutions. This report did not seek to prescribe a single model, but rather to contribute to a broader conversation about responsible data and digital governance for student equity. The findings also highlight several areas where future research is urgently needed to inform more inclusive, transparent, and accountable practices.

7.3 Findings

7.3.1 Framing the analysis: Introduction and structure

The interviews conducted for this research offer a rich and detailed picture of the significant challenges equity practitioners and senior leaders face in achieving effective, transparent, and accountable data and digital governance across the varied domains of their work. While

this report cannot fully convey the depth of these insights, future publications emerging from this Fellowship work will explore particular issues in greater detail and within more targeted contexts. For example, participants raised complex governance concerns specific to institutional disability support units—areas that warrant dedicated attention beyond the scope of this report. Although many of these insights are included here, they are not fully developed.

The central findings have been organised into two distinct categories: high-level themes concerning data and digital governance more broadly, and themes shaped by recent government policy developments. The first category comprises high-level, cross-cutting themes that emerged consistently across interviews. These themes reflect participants' views and experiences of data and digital governance at the intersection of meso- and micro-level institutional practices. The first five of these themes (in Sections 7.3.2–7.3.6) explore the primary concerns and challenges participants identified in how student data are governed and used within their institutions:

- Section 7.3.2 Low institutional data governance maturity
- Section 7.3.3 Local good practice and committed gatekeepers: Commendable efforts, structural concerns
- Section 7.3.4 Shortcomings of data governance models
- Section 7.3.5 The policy–practice gap
- Section 7.3.6 Staff concerns about transparency in student data use

These are followed by two themes (in Sections 7.3.7 and 7.3.8) that explore the common aspects of effective governance that participants frequently identified:

- Section 7.3.7 Centring students as partners in data and digital governance
- Section 7.3.8 Equity-focused leadership: A foundation for ethical data governance

These more positive and constructive themes are further developed in the final two, policy-focused themes (in Sections 7.3.9 and 7.3.10).

Since most interviews were conducted in the second half of 2024, the Accord process, and its associated reforms and debates, featured prominently in participants' reflections. While the Accord's call for enhanced equity data collections has already been discussed, other significant developments were also frequently referenced. These include the government's proposals for needs-based funding, managed growth, the SfSP, and the growing institutional adoption of the SEHEEF equity evaluation framework. Each of these policy shifts carries important implications for how student equity data are collected, acted upon, and governed. These themes are explored in:

- Section 7.3.9 The Support for Students Policy and at-risk monitoring
- Section 7.3.10 Governing equity evaluation: A growing institutional challenge

Shaped by the evolving policy environment, these themes featured prominently in nearly all 21 participant interviews. The first concerns the increasing use of data-driven and digitally enabled systems to identify students "at-risk"—including learning analytics, predictive analytics, and risk dashboards—an area of renewed sector-wide focus driven by the SfSP. The second captures widespread concern about the intensification of data production, analysis, and reporting requirements introduced by current and proposed government policies. In particular, the sector-wide adoption of the SEHEEF was frequently discussed,

and participants raised questions about how student equity data are governed and used in institutional evaluation and quality assurance processes.

Finally, many participants described working in institutional environments characterised by significant organisational restructuring, often linked to budget constraints. At the time of interview, participants were variously anticipating, experiencing, or recovering from restructuring processes. This context is evident in the themes that follow: participants highlighted the serious and ongoing impact of frequent restructures on the capacity of institutions and functional areas to build healthy, stable, and sustainable data and digital governance cultures.

7.3.2 Low institutional data governance maturity

While data governance has become an increasingly important concern in higher education, many institutions remain in the early stages of building coordinated and effective governance frameworks, particularly in relation to equity-related data. Despite the presence of formal policies or committees in some cases, implementation often lags, resulting in fragmented responsibilities, unclear roles, and ad hoc decision-making.

The disparity in relative levels of data maturity is seen in university systems globally. A recent UK study concluded that:

> Universities are at different levels of data maturity, with some having developed functional data warehouses and data governance regimes, while others are still managing disparate databases and low data integration and quality. (Komljenovic et al., 2024, p. 5)

This pattern is not new, nor is it limited to the UK context. Writing about universities in the United States, Borgman (2018) observed that while data governance presents challenges across all institutions, universities face a distinctively complex set of responsibilities and risks in this regard (p. 368). On governance mechanisms specifically, Borgman was pointed in her assessment: “Governance mechanisms to assure protection of privacy … information security, and compliance with regulations in the uses of such data are nascent, at best” (p. 371).

Participants in this Fellowship study predominantly described their institutions’ data governance maturity as low, particularly in relation to equity-related data. Even where formal structures or policies exist, they are often perceived as underdeveloped, inconsistently implemented, or disconnected from day-to-day practice and decision-making. Governance arrangements were often described as fragmented, with unclear lines of responsibility and limited visibility into who has access to which data and for what purposes that access has been granted.

One executive reflected candidly on the disjointed and siloed nature of data responsibilities and the overall immaturity of their institution’s data governance systems:

> I mean there’s different parts of the university that, in theory, have got responsibility for this. And, you know, speaking very candidly, which I am comfortable doing … So, I don’t think our data governance has got to a very mature state in relation to this. (Executive)

A similar concern was voiced by another senior leader, who pointed to the absence of clarity about access protocols and the competing imperatives of support and confidentiality:

> But probably, like many institutions, we're not really great at having total visibility regarding who sees what and why and assuring ourselves that that both maximises the support available for students while respecting their rights to confidentiality. And I mean, I think it's … Let's say it seems just a little bit haphazard. (Executive)

Others framed the problem in terms of inconsistent infrastructure and varying access to data across teams. As one director explained:

> Each piece of that data is different in terms of what our teams can access, or see, or not see. So, [our university] I would say, is at a relatively early stage in terms of its digital infrastructure and it's at an even earlier stage in terms of its data governance, particularly in relation to equity data. (Director)

In some cases, concerns extended beyond governance structures to the reliability and integrity of the data itself. One participant observed:

> I've worked at [many] universities … and this is the one where I would be most concerned about data storage usage and governance. It seems like we can't even rely on the data that we have to be correct. But if you've been there for a long time and you know how to operate the system, you can get in and get the data one way or another … And there was no sort of training around what you should and shouldn't do. And to my knowledge, there's no hierarchy of governance around … who can do what. (Manager)

These reflections point to a substantial implementation gap. Even where governance frameworks exist on paper, participants frequently described a lack of integration into practice, minimal role clarity, and little evidence of cohesive oversight—especially in relation to sensitive student data. As the next subsection shows, some teams, and individuals, have nonetheless taken proactive steps to strengthen local governance practices, although often without centralised guidance or support.

*The low governance maturity and role ambiguity described here justify **R4** (privacy-by-design, role-based access, retention, and audit), **R5** (clarify authority and cross-references across the policy suite), **R7** (formal participation to surface blind spots), **R8** (executive authorising environment), and sector consistency via **R3**.*

7.3.3 Local good practice and committed gatekeepers: Commendable efforts, structural concerns

While most participants described their institutions' data governance maturity as underdeveloped or fragmented, some pointed to examples of localised excellence, instances where committed individuals or small teams enacted strong data stewardship despite limited organisational guidance or support. These efforts were often driven by personal ethics, professional caution, or a strong equity commitment, rather than by formal policy.

As Popescu et al. (2024) noted in their study of data professionals in higher education, such work often constitutes a form of "local privacy activism", data work that "pushes against the

constraints of organisational roles" (p. 11). These are acts of governance by necessity, not by institutional design.

One director described their effort to build a small, dedicated team with both data and equity expertise, aiming to foster a local culture of good practice within a broader institution where such an ethos was largely absent:

> I have really wrestled quite hard over many years to build this very small student evaluation team of people, including qualified academics, who understand data and also who have a very strong equity lens …we've got this little patch of concentrated expertise in the way that we make all of our information asset decisions, in the way in which we shape all of our dashboards, in the way in which we're thinking about who can see what and should there be a filter with the demographic [indicators] or not. (Director)

A senior executive similarly acknowledged that strong governance practices do exist, but tend to be isolated and tied to individual expertise or leadership:

> And look there will be, *absolutely*, pockets of excellence at [the university] that I'm not representing because there'll be people who live and breathe this stuff. There is some really, really rigorous practice. (Executive)

In other cases, individuals were described, or described themselves, as institutional gatekeepers. One participant described a senior data steward who, in the absence of formal governance frameworks, became the de facto ethical decision-maker for student data access—serving as both gatekeeper and single point of failure:

> So unfortunately, we've just had a bit of disruption … [the key senior data steward left the university] and it sent the data into absolute chaos. But when [they were] here, [they] really took it very personally. That if things go wrong, it's [their] job on the line. (Director)

This participant described a longstanding, informal agreement with the steward, built on mutual trust and personal history, through which sensitive data releases were informally reviewed:

> We had an arrangement that I would share any data that I thought might be sensitive with [them] beforehand … it was like a second layer of checking … do you think this is all right? (Director)

While the steward's role had been valued, their departure revealed how dependent the institution had become on one individual's sound judgement. What appeared as good governance was, in fact, a fragile workaround—a substitute for the absence of policy, shared accountability, or role-based access controls.

These governance burdens are not borne by senior staff alone. Several junior participants, particularly those in analytics and evaluation roles, described being left to make important, ethically grey data-sharing decisions without support or clear institutional guidance. As one equity-focused analyst noted:

> I guess a lot of it is me deciding whether they're allowed to have it, and that's probably not in any way the way it should be … Generally, it's up to me to decide whether I agree with sharing that information. (Professional)

In the absence of formal guidance, they had created their own safeguards—including a self-authored data-sharing "agreement" that requesters are asked to complete before receiving data:

> I've instigated my own little statement … just to say that [I'm] not personally responsible for what they do with the data … particularly with stuff that might be a bit more identifiable. (Professional)

Requests from senior leaders are particularly fraught in the absence of clear guidelines:

> I can't say "no, I can't give it to you" because it's come from [a senior person] …there are some things that I'm not allowed to say no to because of where I sit in the food chain. (Professional)

These accounts highlight the institutional risk-shifting that is often at play—where responsibility for ethical data decisions is pushed down to individuals who lack both formal authority and institutional protection. Such patterns suggest that pockets of good practice should not be mistaken for signs of governance success. Rather, they are often acts of self-protection**,** ethical improvisation, and quiet resistance in the absence of well-functioning data governance systems.

Several participants spoke candidly about the personal costs of raising concerns about data privacy and governance practices with senior leadership. One manager said:

> And can I say that this has been very costly for me raising these concerns, right … It's been very costly … It's really, it's very distressing as you could imagine because [I have a long] history of working in this space and it is of great concern to me. (Manager)

Such reflections underscore the fragility and inequity of relying on localised stewardship in place of systemic governance. In the absence of strong policy, clear oversight, and shared accountability, staff are left to navigate ethical tensions alone, sometimes at significant personal and professional risk.

*Reliance on individual "gatekeepers" is fragile; codifying good local practice through **R4** (standard controls), **R5** (institution-wide rules and decision rights), and **R8** (safe escalation, protection for staff) converts personal ethics into durable governance; **R7** embeds lived-experience input, and **R6** provides a proportionate review path for evaluative uses.*

7.3.4 Shortcomings of data governance models

Enterprise data governance frameworks have become increasingly prominent in Australian universities. As found in Section 6, and judging from the presence of data governance policies and frameworks, just under half of all public universities have initiated frameworks of this type. These models, often shaped by corporate logics, seek to manage data as a strategic asset through risk management structures and formalised roles. Yet as participants in this study described, these frameworks frequently fall short of their promise.

Despite formal role definitions, data governance responsibilities are often poorly understood, inconsistently applied, and misaligned with daily practice. Participants reported a policy–practice gap: student-facing staff routinely make consequential data decisions with little ethical guidance or support. In some cases, this disconnection reinforces risk-averse

behaviours, procedural workarounds, or an over-reliance on informal norms (Popescu et al., 2024).

Recent work by McNicol et al. (2024) based on research at the University of Queensland affirmed this broader pattern. Their study found that while data governance frameworks in Australian universities may define oversight roles and establish formal data-sharing agreements, these instruments often suffer from limited uptake, unclear responsibilities, and inadequate visibility. As McNicol et al. (2024) observed, staff may "circumvent existing processes in the interest of progressing their work", not out of disregard for ethics, but because the frameworks fail to accommodate the realities of institutional practice and relational data use (p. 2258).

The following examples illustrate how these limitations play out in practice, across institutions at different levels of governance maturity, and from the perspectives of both data users (equity practitioners) and senior custodians or stewards.

Stewardship governance models across institutions were described by participants as highly uneven, ranging from opaque to nascent, with just one case described as relatively well-functioning. Several participants occupying director-level roles offered insights into these differing levels of maturity. Representing the opaque or poorly socialised end of the spectrum, one director, when asked whether they knew who the data steward is for information central to their role, responded:

> I don't know. No, I mean, who's ultimately signing off on this? I don't know. It's probably the COO or like the, I think the central data area sits under the Chief Operating Officer. And that's where these decisions appear to go, and perhaps legal usually. So back of house, which is interesting. Yeah, these decisions probably don't go through [senior academic staff] … So yeah, it's best not to think about it too much! (Director)

The comment captures a common experience in institutions where governance structures are formalised in name but remain obscure or irrelevant in practice. In this case, the participant also questioned the logic of locating final authority over student and learning data within a "back of house" business unit, suggesting that such governance responsibilities should more appropriately sit within academic portfolios.

The above comment also describes a heavily centralised model of data governance as opposed to a more federated model (discussed in Section 6.5). This participant's comment reflects a common critique of centralised governance models, particularly in universities, where stewardship roles are often horizontally disconnected from the relational and pedagogical contexts in which student data are generated and used. In such cases, governance risks becoming a procedural abstraction: unacknowledged, unowned, and misaligned with core educational priorities.

Even when data stewardship models are known and relatively well established, participants described practical limitations that undermine their effectiveness in both centralised and federated models. A recurring theme was the vertical disconnection between data stewards, often positioned "at the top of the food chain", and the micro-level contexts where sensitive data are a daily feature of equity work. One manager explained:

> And so, I think across the entire university, the only people that really have some hardline about data are the data stewards right at the top of the food chain. They are

> the ones who … will then put these … barriers on accessing [the data] or ensure that we are doing things … the right way.
>
> But it's not until you get to a point of, I don't know, some sort of breach or someone's wanting some data or some information about something that you are then given all these documents about … this is the policy … this is what you need to do. These are all the steps that you need to take. But in terms of practice, you know like daily everyday practice and how people look after all of this information? Yeah, it's pretty bad. (Manager)

This account highlights the procedural rigidity and episodic enforcement that can characterise even mature governance models. When policies and controls are only invoked in moments of crisis or formal request, rather than integrated into everyday practice, stewardship becomes a compliance mechanism rather than a support structure. For practitioners engaged in relational and equity-focused data work, this reactive and top-heavy model can feel obstructive rather than enabling.

Even those who hold senior data governance roles, such as data stewards, custodians, and asset owners, mostly expressed discomfort with the governance model and the institutional supports and mechanisms available to them. One director described receiving frequent access requests through what they see as an outdated and inadequate mechanism, lacking key contextual details:

> The mechanism through which they request that is very clunky and old fashioned and misses all kinds of important questions—like, what will happen if I agree to that asset request? Who will see the data beyond the person asking? What will they do with it? And more importantly, what are the datasets they are hoping to connect it to? (Director)

Although governance responsibilities are formally defined, the participant noted that the broader system lacks "overarching expertise and governance", and that institutional immaturity has limited the development of coordinated, cross-cutting solutions. In the absence of system-level support, decision-making is left to the individual custodian's judgement: "It's dependent currently on the data custodian having a thoughtful, critical, and informed view of how data should be used and who should see it." The result, as this director suggested, is a shifting and inconsistent governance environment, one in which new leaders in areas such as student administration or equity can reshape norms and expectations without those shifts being captured or communicated in any institutionalised way.

Taken together, these accounts reveal that even where stewardship structures exist on paper, they often fail to function in ways that support ethical, effective, and inclusive data use. When data governance is siloed, opaque, or overly reliant on individual discretion, it becomes difficult to navigate, easy to bypass, and poorly suited to the evolving priorities of student-facing work. What is missing, participants suggested, is not only technical clarity but also governance that is contextually attuned, consistently communicated, and embedded in both policy and practice.

*Heavily centralised and opaque frameworks that activate only in crises underscore the need for **R5** (harmonised, auditable end-to-end policy architecture with clear decision rights), **R4** (risk-based controls and PIAs in practice), **R7** (co-governance to align rules with real workflows), and **R3** (national baseline to lift consistency).*

7.3.5 The policy–practice gap

Across the higher education sector, universities have made visible efforts to formalise their data governance through policies, strategies, and digital infrastructure. These frameworks often articulate strong normative commitments to ethical, responsible, and student-centred data use. However, participants in this study consistently described a disconnection between these formal commitments and their practical application in everyday institutional life.

As Komljenovic et al. (2024) observed in their study of UK universities, even when data strategies are well developed, their implementation often falters at the level of practice. Participants in their research reported that data-driven aspirations are frequently undermined by unclear objectives, under-resourcing, fragmented infrastructure, and limited staff capacity to act on data insights (pp. 5–7). Institutional policies, they found, are commonly seen as symbolic or performative, more aligned with compliance or reporting obligations than with the practical realities of teaching, support, or equity work.

Wong et al. (2024) provided further context for why these gaps persist. They argued that data governance is uniquely difficult because of how data are co-created, easily shared, and shaped by systems that often lack clear boundaries or ownership. In their view, governance models tend to overestimate individual control and underestimate the need for collective or contextual approaches—leading to frameworks that are difficult to enact in practice (pp. 3–4).

The accounts that follow illustrate how this gap between policy and practice manifests across diverse university contexts—from unclear or inaccessible guidance to inconsistent application of policy, to reliance on informal norms in ethically ambiguous situations.

Participants described a lack of clarity and consistency in how institutional policies are expected to guide the handling of sensitive data—particularly data linked to equity cohorts. In many cases, staff relied not on clear policy direction, but on informal norms, fragmented processes, or the technical limits of existing systems. One director, when asked how access to sensitive equity data is governed, indicated that policy plays a role, but practice is also influenced by the inherent limitations of the university IT systems:

> Yeah, I think it'll be a combination [of policy and IT constraints]. I do feel like we will have some bits in policy that speak to this, but I don't know if it would go down to the … like we know it's an issue I've talked about with other colleagues around that. It should be role-based [access or permissions] … [But it isn't yet] Which is a failing of the system, but everyone would like to get to that idea that you know, okay, you're [in this role] that means this and then if I stop being that and start being something else, then my access profile should change. (Director)

This comment highlights a core implementation gap: while role-based access to data is widely recognised as best practice and often outlined in policy, IT systems frequently fail to support it—or, in some cases, make it unworkable.

Even at senior levels, participants expressed uncertainty about whether their institution has a data governance policy that informs the decisions of senior stewards, custodians, and asset owners. One director reflected:

> Look, I suspect [the university] would have something with that title … but there isn't really anything that shapes the way you should … have those broader discussions about how we're getting consent and then what are the parameters through which a particular dataset should be used. It feels like it is very much left currently up to individual institutional leaders, to have enough insight or expertise. Or, you know reflexivity, I guess on their own practice to seek a thoughtful, measured, and informed outcome. (Director)

Other participants were more direct in their assessment: institutional policies are not merely unclear, they are irrelevant to how work is actually carried out at the micro level. As one manager put it, formal rules often serve more as symbolic gestures than as practical guides:

> There's a gap between what is rhetoric and what is … well, *it's just rhetoric*. What is stated around, you know, you'll see lots of things where this is what's meant to happen … these are the rules. What the practice is, is not what is clearly stated in the rules. There's no connection. It's fully known. It's not like, whoops … there's a gap! It is like, you know. (Manager)

Here, the participant described not a failure of awareness, but an institutionalised disconnection: a known and accepted divergence between formal policy and operational reality.

For staff working in student support contexts, particularly disability and counselling services, the policy–practice gap is often shaped by deeper tensions between institutional data governance and professional ethical frameworks. In multidisciplinary teams, participants described ongoing disputes over whether internal policies can, or should, override the norms of clinical confidentiality. One director explained:

> [We frequently have the problem of] whose data is it? … that's been coming up in both our disability and our counselling team, we have a lot of clinicians of various types … obviously counsellors … and OTs [occupational therapists] and different kinds of clinicians, social workers that come in to work in these teams … and we have policies and procedures that are quite strict … But we're also in [an organisational area] with these multiple teams supporting a student moving through and everyone's, you know, trauma informed now, so we can't repeat our stories. So, we've had these kind of challenges where an individual team is like [no, you can't have any of this data] … Whereas [the university] wants a bit more flow. (Director)

This quotation reflects a deeper contest over ethical authority and professional autonomy. As Anthony and Stablein (2016) noted, clinical professionals often see confidentiality as integral to their professional identity and are more likely to resist data-sharing practices that conflict with this ethos (pp. 210–211).

In contrast, organisational data governance may prioritise integration and efficiency, creating a disconnection when professional and institutional standards clash. These tensions are compounded when staff work across disciplines governed by different standards and codes, as is often the case in equity work. As Stone et al. (2005) found, even in highly regulated environments, staff often lack clarity on institutional policies and rely on informal norms or professional instincts when navigating data-sharing decisions.

These findings highlight that institutional data governance frameworks, no matter how comprehensive on paper, cannot resolve fundamental tensions between diverse professional

obligations, organisational priorities, and deep personal ethical commitments unless they also grapple with the social and cultural contexts in which data decisions are made.

Foster et al. (2018) argued that the value and risks of data work are negotiated at the micro level, but are fundamentally shaped and constrained by the structural conditions that exist at the meso level, including organisational data governance frameworks, and at the macro level, including law and regulatory policy (pp. 1415–1416). Where meso-level governance frameworks fail to accommodate the professional commitments, relational contexts, and ethical complexities of micro-level practice, a gap between policy and practice is a structural consequence rather than simply a failure of individual compliance.

Closing the gap between policy and practice will require more than clearer rules; it calls for governance that is attuned to the social and professional contexts in which data decisions are actually made.

*This disconnection between rules and reality calls for **R4** (operational privacy-by-design: role-based access, PIAs, audit), **R5** (harmonised, cross-referenced policy suite with clear decision rights), **R7** (co-design and participation to make policies workable), **R8** (executive resourcing and safe escalation), and—where evaluation sits outside HREC—**R6** (defined oversight pathway).*

7.3.6 Staff concerns about transparency in student data use

Participants in this study frequently raised concerns about how clearly students are informed about the ways their data may be collected and used within the institution. Although privacy notices are technically in place, many participants questioned whether these notices are accessible, understandable, or meaningful to students—particularly when consent is assumed rather than actively given.

These concerns closely echo those raised in the *Privacy Act Review Report 2022* (Attorney-General's Department, 2022) and reviewed in Section 5 of this report concerning transparency and the ambiguity of consent. Participants noted that such practices may disproportionately affect students from equity groups, who may be less likely to trust institutional processes or feel empowered to question how their data are used.

Participants highlighted a disconnection between formal privacy collection notices and students' expectations about how their data will be used. One senior executive noted that their university's privacy policy—like those of all Australian universities—permits the collection and use of sensitive student data for broadly defined institutional purposes, but worried that, although these practices are technically disclosed, students rarely scrutinise them at the point of agreement: "It's kind of like a terms and conditions thing. I think people just go: 'Yeah, yeah, whatever.'" (Executive). The participant then described an instance of inviting student participation in data governance processes, noting how students' perspectives shifted once they were engaged more directly with the topic:

> You saw a greater level of interest on, "well, would my academic know that I'm neurodivergent because I don't know if I want that", and so we had to kind of work through how we control that through access and inclusion. (Executive)

In the same interview, the executive reflected on the institution's internal governance arrangements, admitting that while students are nominally informed of data practices through

policy statements like those reviewed in Section 6, internal mechanisms to ensure clarity and accountability are underdeveloped: “But my view is that it’s probably not explicit and clear enough about how we, how we govern that across the institution and it’s a bit slippery” (Executive).

Another senior participant echoed this view and worried that while central privacy policies and collection notices mean that “we’re allowed to use student data for the purposes of the university’s business”, the use of these data for research and intensive evaluation purposes is less transparent. In this respect, the participant reflected, “I think we need to be more robust in the way in which we evidence voluntary and informed consent for the use of those data” (Executive). Together, these reflections suggest that even when disclosure occurs, it often does not result in meaningful understanding or engagement.

Many participants in this research were particularly concerned with the transparency and ambiguity surrounding data collection related to disability disclosure. Several staff reflected on how students are often asked to indicate a disability status during enrolment or support registration processes without being given a clear understanding of the consequences, including who might access that information, in what context, and for what purposes. One director expressed this concern directly:

> And I think one of the principles that I think we’re trying to hold fairly clear is that students should know about the data the university is holding in relation to the student. And in fact, students should be *very* aware … we’ve literally been looking at disability in exactly this lens. They should be aware of what them ticking “Yes” in a box will mean and what it won’t mean. And I think that clarity is really crucial to the student feeling that they have got some agency within their educational experience. (Director)

Disability support practitioners were also acutely aware of the volume of informal, sometimes undocumented, data practices that sit outside formal policy disclosures. Several referenced the routine use of case notes, email trails, and document uploads in institutional systems that track student interactions—often with no obvious transparency to students themselves. One professional working in disability support questioned the ethics of these practices:

> But are we telling students [with disability] that … we grabbed their emails that they send, and we put that into the case management system? You know, our [staff] do that so we’ve got this history of … correspondence and everything else because there might be a different [disability adviser] that does that or it went off to enrolments and there’s an email, but who does that sit with? Does it get captured? [Have we made] the student aware that anything they’ve emailed into us is captured in the system and sitting against their name? [Do they know] we’re keeping their data? Do we tell them any of this? Yet, “we’re big on privacy!” (Professional)

These reflections point to a recurring concern among participants: that student consent and institutional transparency are often murky or overly reliant on broad notions of implied consent. While students may technically “agree” to data collection and use through enrolment forms or standard privacy notices, participants questioned whether such mechanisms meaningfully supported informed or voluntary consent—particularly in cases involving sensitive data, such as disability disclosures.

These insights similarly reflect the conversations relating to the ongoing reforms of the *Privacy Act* and the pressing need for clearer and more meaningful consent and other protections outlined in Section 5.

*Murky notice or consent and unclear use of sensitive equity data point directly to **R4** (stronger APP-5 notices, active consent where appropriate, ADM transparency), **R5** (align privacy, data, AI, and support policies), **R7** (student and staff co-governance of notices and data uses), **R8** (leaders to model and resource privacy by default), and system-level uplift via **R3** (national templates and baselines) alongside **R1**–**R2** (policy guardrails and funding levers).*

7.3.7 Centring students as partners in data and digital governance

Across all interviews in this study, participants expressed strong support for involving students more directly in the governance of data and digital systems that affect their educational experience and their personal information. Whether framed in terms of ethical responsibility, institutional transparency, or the practical value of lived experience, the principle of student participation was consistently endorsed. While views differed on how such involvement should be structured or scaled, there was clear agreement that student perspectives are essential to fair, accountable, and responsive data governance. The accounts that follow illustrate both the motivations behind this view and the practical possibilities participants saw for meaningful student inclusion.

Several participants went beyond endorsing student involvement in principle to describe concrete, well-resourced models of participation in governance processes. One senior leader explained:

> I deeply feel it is crucial for universities to incorporate student voice. And I have particular views on how that should be done. And [I believe] we should be paying student partners in order to draw on their expertise within our key governance structure. [This is something we have done on a large project that] was absolutely shaped by student voice. And I think it's so, so completely crucial. And I think it's the only way for universities to go if we're going to be really serious about making these decisions well. (Director)

This example highlights a growing recognition that genuine student participation requires not only consultation but sustained engagement, appropriate resourcing, and institutional commitment.

The motivation for paying students is also telling and seeks to address one of the often-cited problems with some students as partners models. As the same participant noted, student governance positions tend to attract "highly motivated student[s] with lots of social capital", who may not reflect the diversity of the broader student body:

> Often the people who can afford to spend their own time just attending those meetings … are quite different from the students who need to be paid for their time. (Director)

For this reason, they argued, payment must be "the starting point" for any serious and inclusive approach to student participation in governance.

One senior executive described a shift from retrospective consultation to genuine co-design in projects involving learning analytics and data-intensive predictive analytics use cases. In a current initiative focused on identifying students "at risk" of not completing a unit, they emphasised the need to "centre students in the conversation about what's going to trigger an intervention". While acknowledging that policy development has traditionally involved students only at the consultation stage, they noted a growing institutional commitment to involving students earlier and more meaningfully: "More and more we are developing things with students in the room in the first place, which is what co-design is" (Executive). Their institution, they explained, now routinely incorporates student advisory groups into projects involving learning analytics, GenAI, and broader digital governance work.

Across these accounts, the message was clear: early, meaningful, and well-supported student partnership was seen not only as desirable but as a necessary foundation for good practice in data and digital governance.

*These findings point squarely to **R7** (embed representative student participation and co-design in data governance), enabled by **R8** (executive resourcing and authorisation), and embedded via **R5** (codify participation in policy and charters with clear decision rights). Sector scaffolding from **R3** and **R9** can supply common templates and practice standards.*

7.3.8 Equity-focused leadership: A foundation for ethical data governance

Before formal policies take hold, meaningful change is often catalysed by an influential individual—trusted, principled, and equity focused. In the few cases in which participants described more mature data and digital governance, they credited institutional champions, deputy vice-chancellors, chief operating officers, or respected researchers, who prioritise ethical, equity-centred data use and align fragmented efforts. These champions matter not only for their authority or expertise but for values-led leadership: centring student equity, navigating institutional tensions, and converting intent into strategic, coordinated action.

This kind of leadership resonated with Bonawitz et al. (2020), who argued that champions must offer more than positional power—they must bring credibility, relational presence, and a clear sense of purpose. Shea (2021) similarly emphasised that it is sustained commitment, grounded expertise, and visible organisational support that enables champions to foster trust and effect change. The following reflections illustrate how participants experience this equity-driven leadership in practice—leadership that bridges silos, builds shared purpose, and stewards emerging data cultures with care and clarity. It should be noted, however, that illustrative quotations in this section are intentionally limited to avoid identifying participants or their institutions.

One participant in this research was particularly optimistic about their university's capacity to develop effective, equity-centred data and digital governance policies, practices, and cultures. This optimism was largely attributed to two factors: the presence of several senior academics with expertise in closely related research fields, and an institutional ethos that prioritises equity. The participant described how this combination of leadership and values has fostered a coherent and ethical approach to governance:

> I've been very glad to have worked very closely with [this academic leader because] they make sure [data and digital governance efforts] are equity centred and [they

> bring] that lens and also talk about the ethics around it. It's about being student centred as well. (Manager)

They went on to emphasise that the university's culture of ethical awareness and student equity runs deep:

> Equity-centred, student-centred, and thinking of the ethical implications. That drives the kind of work that comes from [the university]. So yeah, in terms of my thoughts, I think we've been heavily guided by [this academic leader] around all of this. But we've not had to, you know, be critical or say anything much around it, because that's [their] natural default as well. Like, [they will] talk about the ethical implications for equity cohorts. So, that … helps because that also aligns with the data governance and policies we have. (Manager)

Anderson and Diamond (2020) argued that meaningful Indigenous leadership in university governance is critical for achieving justice, structural inclusion, and culturally responsive institutional practices. This assertion strongly aligns with a theme raised by several participants, who particularly highlighted the influential role of senior Indigenous academic leaders in embedding ethical governance within student support strategies and data practices. Participants underscored that the involvement of these leaders is not merely beneficial but foundational—enabling approaches to data governance that are respectful, contextually grounded, and genuinely responsive to Indigenous community priorities.

One participant, who holds a senior role focused on Indigenous strategy and governance, described how sustained efforts over many years have resulted in a well-developed, institution-wide structure they characterised as "a very comprehensive Indigenous governance mechanism" (Executive).

While only limited quotations can be shared because of the risk of identifying individuals or institutions, the participant underscored the pivotal role of several senior Indigenous academic leaders—respected scholars with national and international standing—who have shaped the university's approach to the governance and use of student data.

They described how the institution's "comprehensive Indigenous governance mechanism" has evolved into a deeply data-informed framework that establishes clear targets and monitors progress towards Indigenous student participation and success. According to the participant, this framework has been carefully developed and continually strengthened over many years, driven by the sustained leadership of Indigenous academics recognised for their expertise in data-intensive research domains and Indigenous data sovereignty.

This longstanding leadership, combined with robust governance and Indigenous oversight, has cultivated an institutional culture whereby student data can be managed confidently, ethically, and sustainably. Rana and Azeez (2025) reinforced this perspective, arguing that meaningful advancement of Indigenous data sovereignty in higher education requires more than symbolic reform; it necessitates placing First Nations leadership, control, and knowledge systems at the centre of institutional governance.

While participants did not specifically speak to the presence of senior data and digital governance champions with lived experience of disability, the absence of such leadership was notable—especially when contrasted with recent policy following the Accord. Harpur et al. (2025) provided a powerful example in their critique of the Accord final report, where flawed disability data and deeply problematic assumptions, such as excluding students with

“profound” disability from participation benchmarks, led to weak, even regressive, policy recommendations. They argued that such outcomes are symptomatic of decision-making processes that lack authentic disability leadership.

The authors proposed a disability-led, sector-wide inclusion strategy grounded in the principle that people with lived experience must shape the frameworks, data cultures, and governance processes that affect them. As Harpur et al. (2025) argued, “a disability equity and inclusion policy cannot be created unless people with a disability are at the leadership tables” (p. 4).

The absence of senior leaders with lived experience of disability in data governance and equity forums is not a minor oversight but a structural gap that undermines inclusive policy. Addressing the gaps in First Nations and disability leadership is therefore imperative: if data governance is to advance inclusion and justice rather than reproduce inequities, leadership must reflect and be accountable to the communities most affected by data practices.

At the same time, participants and scholars alike warned against the risks of over-relying on a small number of individual champions. While these leaders play a crucial role in driving meaningful change, their influence must be institutionalised through formal, university-wide structures and practices that embed data and digital governance explicitly centred on equity across diverse roles and sustained over time. This is seen clearly in the earlier example of individual Indigenous leaders being instrumental in initiating change, resulting in a “comprehensive Indigenous governance mechanism” that is distributed, sustainable, and positioned to continue the work of institutional change.

*The value, and limits, of individual champions underscore **R8** (leaders to resource, authorise, and model privacy by default), with **R7** (ensure First Nations and disability leadership in governance), and **R5** (institutionalise beyond individuals through harmonised, cross-referenced policy). Sector-level support via **R3** and **R9** can stabilise these gains.*

7.3.9 The Support for Students Policy and at-risk monitoring

The use of student data for digital at-risk monitoring, particularly in relation to equity cohorts, emerged as a significant concern among participants in this study. Given its prominence, this issue is examined in a dedicated subsection but remains closely connected to broader themes of governance, ethics, and student equity explored elsewhere in the report.

As the review of SfSPs in Section 6.5.3 found, most policies confirm that proactive in-semester monitoring is occurring, but few specify the data sources, analytic methods, or governance arrangements that underpin it. This gap between policy imperatives and institutional readiness to meet the associated governance demands was keenly felt by participants in this study, many of whom were directly involved in implementing or overseeing these systems at their institutions. Several identified the SfSP as a key driver behind efforts to expand data collection and accelerate the development of academic early-warning systems:

> So, this year we’ve accelerated [our development of at-risk analytics] because of the Support for Students Policy, and we were quite behind the eight ball. As of this year, we are using LMS data … globally across the whole student population. […] In prior years we’d done various pilots, but this is the first time we’ve really scaled up. (Director)

As with the SfSPs reviewed in Section 6.5.3, the participants in this research voiced considerable variation in how risk is described and operationalised. Terms such as “suitability”, “preparedness”, “engagement”, and “progress” are used alongside varying analytic techniques, including “predictive analytics”, “learning analytics”, “at-risk modelling”, and “propensity scoring”. Following the *Higher Education Provider Guidelines 2023* (Chapter 10A, Support for Students Policy), this report adopts the term “at-risk” without presuming a single definition of what that condition entails.

Australian universities have a long history of using digital systems to monitor student progress and engagement (Macfadyen & Dawson, 2010). At-risk systems take diverse forms, ranging from basic rule-based alerts, for example non-attendance or missed assessments, to sophisticated models that use multiple behavioural and demographic variables to generate risk scores (Tsai et al., 2020). As detailed in Section 6.5.3, some predictive systems include equity indicators such as low SES background, First Nations status, or age at enrolment; others avoid such variables because of ethical and reputational concerns (Stephenson et al., 2022), a tension also explored in the discussion of inferred data in Section 4.4.4.

This diversity suggests that at-risk monitoring should be understood not as a single model but as a family of practices shaped by different assumptions about risk, student agency, and institutional responsibility.

Data and digital harms: Both realised and mitigated

The introduction of SfSP requirements has prompted many universities to revisit older at-risk systems, some of which had previously been abandoned or deprioritised. Several participants shared examples in which early predictive models were discontinued because of poor performance, ethical issues, or loss of staff confidence. Concerns were raised that some systems reinforce deficit views by associating risk with demographic characteristics, rather than contextual or structural factors. Participants questioned whether these tools genuinely support students or function more as surveillance mechanisms. One director shared:

> So, when I started, I was getting a list in [academic area] of students I thought were disengaged and was like, “How come the list that the call centre’s contacting is completely different?” They were using predictive analytics, but no one had gone back and checked that the main predictors [were still] being collected within the dataset. So, they were—well, *it was completely racist.* So, they did no evaluation, or reflection, or anything, but every session they just got a list of students at the start of session that were “at-risk” … It just gave them a number. (Director)

The participant was describing a well-documented risk in predictive analytics: when demographic attributes such as Indigenous status are included as model inputs without ongoing validation, they can function as proxies for risk in ways that systematically over-flag entire cohorts, producing outputs that are discriminatory in effect regardless of intent. For a fuller treatment of this issue, see Stephenson (2022).

Like many institutions, this university shifted to using only behavioural indicators rather than static demographic attributes: “So that’s when we started looking at which students were missing an early assessment item pre-census and contacting those students who actually are at-risk” (Director).

Another manager explained their institution's shift away from demographic attributes:

> What we're really trying to get down to is the behaviour in their study … in how they're studying and what they're engaging with … I think [these] can be a better indicator of where they are and what they need. Those things are … a lot more powerful in the long run. (Manager)

A third participant described a two-step process, whereby equity attributes are added to the dataset only after the risk-modelling process is complete:

> But then once they're identified, then we pull information about their demographic background, so it doesn't feed … so we don't make assumptions that they're at-risk by equity status … once they're identified at-risk we [look to see] how many have an equity status. (Director)

These examples reveal an emerging distinction in practice. While demographic data remains valuable for understanding context, many institutions are decoupling it from the initial risk assessment process to reduce bias and avoid reinforcing deficit assumptions. This is an important distinction that students can readily grasp. Making this distinction clear in university policies and communications to students would go some distance towards making data and digital policy transparent.

Poor consultation with practitioners and ethical concerns

Despite being responsible for supporting students flagged as at-risk, frontline staff are often excluded from the overall system design process. Several participants reported being handed lengthy, unexplained lists of students—raising questions about how to intervene meaningfully or ethically. One manager reflected:

> I was not very happy about some of the stuff that they were doing … they're sort of using, moving towards identifying that if a student has a disability, if they come from a low SES area … that they are more likely to not succeed in their studies, which all the research shows the opposite, right?…So, if they've actually been able to get to university in the first place, well … they're amazing because they can actually study by themselves and they know what they're doing. (Manager)

Another raised concerns about the level of system transparency that is provided to staff:

> I'm just working out a process to know what on Earth we're supposed to do with it. There are [several thousand] students on the list at the moment. What are we supposed to do with that? I've been quite cautious about the list. Because I didn't know what parameters were being used to identify students, and I was concerned that equity parameters were built into it and I'm not sure that they are now. (Manager)

These accounts point to a fundamental design problem. Liu et al. (2023) found that predictive systems in education frequently fail when problem formulation is driven by data availability and technical convenience rather than genuine engagement with education goals and stakeholder needs. They documented how naive application of risk scores, without adequate resourcing or intervention design, can stigmatise students and worsen outcomes rather than improve them (pp. 4–6). The experiences described by participants in this study reflect precisely this pattern: without meaningful involvement of frontline equity staff in system design, and without transparent communication of how systems work, at-risk monitoring risks becoming a burden rather than a support for the students it is meant to help.

Governing at-risk monitoring: Participation, privacy, and oversight

Few participants were aware of institutional policies governing at-risk monitoring specifically. Most cited privacy policies as the only applicable framework. Despite a lack of policy, several participants described formal governance mechanisms, such as cross-functional committees or working groups, that play a vital role in oversight, accountability, and ethical review. One executive described their university's governance approach:

> We absolutely need to centre students in the conversation about what's going to trigger an intervention moving forward … we've got a governance structure, [including several staff groups or committees], but there is also a students-as-partners group that will be part of that and has been. (Executive)

This aligns with calls for student co-design in learning analytics and AI governance (Dollinger & Lodge, 2019), and echoes the broader finding in Section 7.3.7 that meaningful student participation requires not only consultation but sustained engagement, appropriate resourcing, and institutional commitment.

The early deployment of cross-functional PIAs was again cited as a practical governance mechanism that ties participation, privacy, and oversight together in at-risk monitoring programs. Conducted before deployment, they convene practitioners and interconnected teams to map data flows, surface risks, agree mitigations, set review cycles, and secure formal approvals. As one manager explained:

> through that PIA process, we had to also talk about the risks around how people are accessing that data. What are the mitigation strategies … how many times throughout the year we review this document … and get approval from the [Privacy Officer]. (Manager)

Taken together, these findings highlight the ethical, practical, and governance challenges associated with predictive analytics in Australian higher education. Effective implementation of at-risk monitoring systems demands technical sophistication alongside equity-centred design, staff collaboration, transparent governance, and formal safeguards such as PIAs. Where universities treat these tools as part of a broader commitment to student wellbeing and inclusion, rather than simply as compliance mechanisms, they are more likely to build systems that are both effective and ethically sound.

SfSP-driven "at-risk" monitoring sits exactly where privacy, equity, and digital practice meet. Making it safe and effective requires: ***R4*** *(privacy-by-design controls, ADM transparency, role-based access, PIAs and model-risk management),* ***R5*** *(harmonised, cross-referenced policy architecture linking SfSP, learning analytics and AI, privacy and data governance),* ***R7*** *(paid, representative student and staff co-design and oversight), and—where monitoring and evaluation falls outside HREC—****R6*** *(a defined, proportionate oversight pathway).*

7.3.10 Governing equity evaluation: A growing institutional challenge

This final qualitative section of the report examines a critical data governance challenge consistently highlighted by research participants: managing the growing demand for rigorous, data-intensive evaluation of student equity initiatives. With interviews conducted largely in late 2024, the Accord process, and its associated proposals and reforms, featured prominently in these discussions. The expectation of enhanced evaluation was articulated in

the Accord final report, which stated that equity-related funding should be linked to robust program evaluation:

> The *Student Equity in Higher Education Evaluation Framework* (SEHEEF), which is in the early stages of implementation, should be leveraged to embed appropriate evaluation and reporting mechanisms … Universities should be required to account for the effectiveness of their activities, but evaluation structures should also enable longitudinal and systemic evaluation of outcomes at a whole-of-system level. (Department of Education, 2024a, p. 130)

Other key policy developments emerging in the wake of the Accord, including proposals for needs-based funding (Department of Education, 2024b) and recent reforms to the Higher Education DSP, reinforce these expectations, signalling heightened accountability requirements tied to equity-related funding.

While the embedding of the SEHEEF (Robinson et al., 2021) was broadly welcomed by participants in this research, many expressed growing concerns about institutional readiness to manage complex data privacy, ethical, and governance demands related to evaluation activities. The intersecting challenges explored throughout this Fellowship, including data governance maturity, transparency, and the ethical use of equity data, provide important context for the concerns raised in this subsection.

The growing pressure to collect equity data of all descriptions

Several of the more junior participants in this research described growing pressure from senior executives to urgently collect data on equity, and equity-like, cohorts. This pressure was often tied to demands for program evaluation or the need to demonstrate compliance with funding and policy obligations set by government. In many cases, the data requested were clear examples of the grey or incidental equity data that was described in this report, with the help of Borgman (2018), in Section 4.4.5.

The experience communicated by one participant is particularly instructive and reflects many similar stories that were shared by others. This participant's role, at least in part, involves running workshops for students with disability. Like many others, the participant described being under "aggressive" pressure to generate new data collections—largely grey data, often paper-based rather than digital, and gathered under conditions of unclear or limited consent—for use in evaluation and reporting to government. Reflecting on recent government policies and the growing pressure to demonstrate both compliance and impact, the participant remarked:

> Everyone's convinced they're gonna have to show evidence for this in like six months … we've gotten this sort of like message from God here that if you're doing stuff [with equity students], you need to generate data for it because they want to see data … Have we talked about this? No, not beyond "just collect it". (Professional)

The pressure for data collection and evaluation, this participant explained, did not come with an equal sense of urgency, on the part of the university, to ensure the responsible governance of what was clearly sensitive health information.

> we've been getting incredible pressure for evaluation because we have [many new senior executives] and their big thing is data, data, data, data, data, but we're getting

> no guidance. None on the ethics of collection, you know, storage, or analysis. (Professional)

The experience of this participant is instructive on several levels, but it usefully encapsulates what many participants across all levels of seniority described as the time- and resource-constrained nature of equity work, and therefore, of data work:

> I don't get support for doing things like ethics applications, and I don't have time to do ethics applications. It's just … it's a real chicken and the egg problem around, give us data, give us data now … [but] we're not gonna give you any support whatsoever in doing it. (Professional)

These reflections highlight a disconnection between the growing demands for evidence and evaluation in equity programs and the limited institutional investment in the ethical, supported, and accountable data practices required to meet them.

These findings serve as an introduction to key themes raised by other participants in this research that should be borne in mind, by all stakeholders, as the SEHEEF is further embedded across the sector. It also raises questions for government about institutional readiness, that is, institutional data governance maturity, in relation to its own expectations for evidence of impact and accountability.

The blurred lines between research and evaluation

As universities face increasing demands to demonstrate the impact of equity initiatives, the distinction between research and evaluation has become harder to navigate. While research activities are subject to established ethical review processes, evaluation and quality assurance practices often operate in less regulated spaces. Participants in this research described how these blurred boundaries create challenges for governance, consent, and accountability, particularly in the use of student equity data.

The *National Statement on Ethical Conduct in Human Research* (National Health and Medical Research Council, 2023, s 5.1.7) requires institutions to establish clear policies that differentiate research from other activities such as evaluation or quality assurance, "and have separate mechanisms for the review and authorisation of each". Despite this, very few participants in this research were aware of policies, procedures, or clear means of seeking institutional authorisation for evaluation activities.

As one participant, who was particularly concerned with the casual use of sensitive student data for evaluation purposes, described:

> Look, there probably is a policy … but people aren't looking to that policy, and I mean who's accountable, right? Who becomes accountable for making sure that that policy is enacted or followed? Particularly, you know when it comes to evaluation, because there's some very clear things when it comes to ethics and research, but evaluation is a different ballgame. And you think people kind of get away with a lot of things when they call it evaluation. (Manager)

Several senior participants echoed this concern. They pointed to gaps in policy, procedure, and culture and stressed the need for stronger and more formalised governance of evaluation. One participant from a university embedding a SEHEEF-informed evaluation culture stressed the need for clearer policies, stronger oversight, and formal approval

processes for both external research and internal evaluation. The participant suggested that a senior data steward should:

> have oversight of every request from a researcher […] to recruit students or to use students' data, because that goes very much into students' learning management system data, their analytics, their evaluations, that is, student evaluations of teaching and units. But also data […] that students don't even know, or data from students engaging with an equity intervention, for example. And then those data, even if they're aggregated, being used in some form of output, I would like to have some quality assurance oversight of that in terms of … organisational consent. (Executive)

Reflecting on equity program evaluation and the murkiness of university privacy notices, the participant added:

> Look, we have all of our privacy statements. You know, we're allowed to use student data for the purposes of the university's business, which fits under that criteria. Certainly, if we're going to then be sharing that information more broadly, certainly publishing, but even sending it back to the government, or who knows where … *I think that we need to be more robust in the way in which we evidence voluntary and informed consent for the use of those data.* Yeah, maybe not more broadly, but for particular programs or interventions, yeah. (Executive)

The policies reviewed in Section 6 reveal that some universities require approval from a senior data steward for any proposed use of student information for research purposes. In very few cases, similar approval is required for certain internal uses of student data. However, such governance processes are extremely rare across the policies reviewed, and as most participants observed, formal mechanisms for securing "institutional consent", outside of HREC review, are often informal, inconsistent, or entirely absent.

Nearly all participants in this study described approval processes for activities falling outside HREC oversight as largely informal. One senior participant captured what appeared to be a common pattern:

> So, if it's [for] an internal purpose, usually the … so on all of our dashboards, they would highlight this information. It's linked to our policy and some guidance around what you can and can't be using it for. But there's certainly no group that you would go to. It's literally myself and [a colleague], and we're kind of the owners of that data and we give guidance. But beyond that, it's not, it's not very sophisticated … But around evaluation we probably haven't thought about it, to be honest. I think it's a really good question in terms of our public reporting on these sorts of things. Yeah, no, we haven't considered that actually. (Executive)

Another executive-level participant expressed deep discomfort with the underlying rationale driving calls for increasingly rigorous student equity evaluation. They raised concerns about the potential for harm, particularly to students who may be unfamiliar with academic research and evaluation cultures, and highlighted the ethical risks of using student data without meaningful transparency or consent. They cautioned:

> we have to really take pause about how often we're using students as potential lab rats in things that, you know, could cause harm … and done at an institutional level, and reflect on the fact that most people running institutions are wealthy now, either by their employment at the university or their own background, and so it's almost again

> […] the wealthy playing around with people from disadvantaged backgrounds, for, I'm not sure, what end? I think we need data evidence, but it needs to be done respectfully, and it really needs to be done with the individual in mind. (Executive)

This comment underscores the need to interrogate not just the technical processes of evaluation but the power dynamics and ethical assumptions that shape them. As universities expand their use of equity data for evaluation and reporting, care must be taken to avoid extractive or instrumental approaches that risk further marginalising the very cohorts they aim to support.

These reflections point to a clear gap in institutional governance: while ethical oversight is well established for research, evaluation practices involving student equity data often fall into poorly defined or unregulated spaces. The absence of formal mechanisms for oversight, authorisation, and organisational consent not only creates ambiguity for practitioners but also raises significant risks for institutions. Equity evaluation is becoming more data-intensive and externally visible, particularly under frameworks such as the SEHEEF. Governance processes must keep pace, recognising the ethical stakes of equity data use beyond traditional research contexts.

*As SEHEEF implementation and related funding settings place growing evaluation demands on institutions, universities need a defined and proportionate oversight pathway for equity-related evaluations, connected to existing HREC processes (**R6**), supported by **R4** (privacy-by-design, PIAs, and role-based access), **R5** (harmonised and cross-referenced policy suite), and **R7** (student and staff participation). System-level levers (**R1**–**R3**) should embed guardrails, enable funding for capability (**R2**), and deliver national baselines and tools (**R3**). Senior leaders should resource and actively champion a privacy-bydesign culture at the frontline (**R8**).*

7.3.11 Reflections and implications from the qualitative study

This qualitative study has illuminated the lived realities of equity practitioners, senior leaders, and data professionals working at the intersection of student equity and data governance. Across diverse roles and institutions, participants identified significant ethical, procedural, and cultural challenges, alongside examples of committed local practice and equity-informed leadership. Their reflections reveal that while policy frameworks continue to evolve, the practical governance of student equity data remains uneven, under-supported, and often ethically ambiguous. As Australian universities respond to growing demands for data-informed evaluation and accountability, these insights underscore the need for governance approaches that are not only technically sound but equity-conscious, contextually grounded, and shaped by those closest to the work—equity practitioners. The following section discusses the implications of these findings and outlines key recommendations for government, universities, and practitioners.

8. Discussion

The findings presented in this report highlight a higher education sector facing intensifying demands to demonstrate impact, support student success, and ensure accountability in equity-related work. At the macro level, universities are navigating increasing regulatory complexity and fragmented legal frameworks, particularly in the context of privacy reforms and evolving national equity policies. At the meso level, institutional policies and data governance structures remain inconsistent and frequently disconnected from operational realities. Meanwhile, at the micro level, the experiences of equity practitioners and senior leaders reveal a landscape shaped by ethical tensions, informal workarounds, and the practical burdens of data collection, governance, and ethical decision-making. Together, these findings point to a sector whose governance frameworks have not kept pace with the datafication of equity practice, and where the governance of student equity data must evolve to meet not only legal obligations but also higher standards of ethical practice, transparency, and inclusion across all levels.

The following recommendations respond to this context. They are grouped by stakeholder audience and framed as high-level actions, grounded in the findings of this Fellowship and aligned with emerging national reforms. These recommendations rest on a central proposition: ethical data governance is not merely a matter of compliance but a condition for advancing student equity in a sector undergoing rapid datafication and digitalisation.

8.1 Recommendations for government and policymakers

R1. The Australian Government Department of Education should embed privacy, data, and digital governance safeguards across the equity policy life cycle—design, implementation, and evaluation.

As new funding models and equity evaluation frameworks are introduced following the Australian Universities Accord—including needs-based funding and the SEHEEF—there is a significant opportunity for the Australian Government to ensure that equity policy initiatives are accompanied by strong data governance safeguards. These safeguards should account for the sector's variable data governance maturity and include meaningful consultation with equity practitioners, privacy experts, and students. Particular care should be taken to avoid data-driven harm arising from rapid growth in equity data collection, especially where governance maturity remains low and risks may be borne disproportionately by students from equity cohorts and frontline staff. Embedding these safeguards across the full equity policy life cycle, from design through implementation to evaluation, would support more equitable and ethically grounded outcomes across the sector.

R2. The Australian Government Department of Education should permit equity program funds to support privacy-by-design, ethical evaluation, and equity data governance capability in universities.

Effective national equity policy depends on the ethical governance of student equity data as a foundational condition, yet governance capability has consistently received insufficient institutional investment. There is a significant opportunity for the Australian Government to explicitly permit a portion of equity program funds to be directed towards practical data and digital governance capability uplift. This investment should support privacy-by-design initiatives, such as consent redesign, secure role-based access controls, and professional development for frontline staff, which are essential to resolving the gap between policy intent and institutional practice evident across the sector. Funding settings should acknowledge that governance maturity varies considerably across institutions, enabling targeted capability uplift rather than assuming a uniform baseline, and thereby supporting the generation of reliable and ethically grounded evidence for equity policy.

8.2 Recommendations for sector steward and regulator: ATEC and TEQSA

R3. ATEC and TEQSA should collaborate to establish a national baseline for student equity data governance and provide shared, sector-specific tools to drive consistency across a fragmented landscape.

The report identifies a structurally fragmented legal and institutional landscape as a significant source of ambiguity and inconsistency for university staff and risk for students. There is a significant opportunity for ATEC and TEQSA, acting within their respective stewardship and regulatory functions, to work together to bring greater consistency to student equity data governance across the sector. Working collaboratively, the two bodies could prioritise the development and publication of shared, sector-specific tools—including adaptable templates for privacy notices and PIAs, and minimum data governance controls—that promote equity-conscious practice while preserving the institutional context in which universities operate. A periodic, proportional sector review could further support consistency over time, reducing unnecessary duplication in local policy development and providing a shared evidence base for ongoing improvement.

8.3 Recommendations for universities

R4. Universities should adopt standards above legal minima and implement privacy-by-design and robust data and digital governance.

Where governance frameworks rely solely on legal minimum standards, they are poorly equipped to account for the full scope of student equity data, including grey, inferred, and incidental data, and the risks these create. Universities should treat privacy-by-design as standard practice and implement a coherent and proportionate set of data governance controls that go beyond minimal compliance. In practice, this means strengthening point-of-collection notices, clearly explaining ADM uses, and embedding a risk-based threshold that triggers PIAs for high-risk or equity-risk projects. It also means implementing proportionate, role-based access controls with auditing and stringent data retention safeguards. Particular care should be taken with small cohorts where re-identification risk is elevated, and formal model-risk management should be applied where analytics are used in equity contexts.

Together, these measures would lift institutional practice beyond the statutory floor, reduce the likelihood of data-driven harm, and better support staff navigating the ethical grey zones that are inherent to equity work.

R5. Universities should harmonise digital and data policy frameworks and centre equity across the policy suite.

Fragmented and unaligned institutional policies are a significant structural contributor to the ethical grey zones experienced by frontline equity staff. Universities should prioritise harmonising their data, digital, and student equity policy frameworks to address this systemic fragmentation. Where policies governing privacy, disability, AI, and analytics are developed and maintained by different units operating in silos, contradictions emerge that create policy–practice drift and hinder consistent decision-making. Harmonisation should focus on removing those contradictions, adopting standard terminology for advanced data-processing techniques, clarifying authority and escalation pathways, and embedding explicit equity-risk statements, roles, and protections across the policy suite. A coherent and aligned policy architecture is not only easier for staff to follow and escalate through, it also ensures that equity considerations are embedded by design rather than addressed as an exception.

R6. Universities should establish defined oversight responsibilities for equity-related evaluation activities that fall outside HREC review.

A significant governance blind spot exists where internal evaluation activities fall outside mandatory HREC review yet increasingly carry data and privacy risks that are not meaningfully distinguishable from those arising in formal research. The research found that some universities had developed local data governance cultures, or relied on individual governance gatekeepers, that partially filled this gap in practice. However, these arrangements were often fragile and informal, dependent on the presence of a single knowledgeable staff member or an invested senior leader. They were therefore vulnerable to being lost through staff turnover or leadership change. Universities should address this by embedding a low-burden, formally governed oversight pathway within or alongside existing HREC processes, rather than creating a parallel structure. This pathway should include a lightweight threshold assessment to triage evaluation proposals, routing low-risk activities through an expedited process while escalating medium- and high-risk projects involving, for example, sensitive or inferred equity data, ADM profiling, or targeted outreach, to full HREC review. Framing internal evaluation within this extended governance pipeline would ensure that the absence of an intent to publish does not exempt an activity from ethical scrutiny, improving both the integrity of evaluation practice and the protection of equity students whose data is at stake.

R7. Universities should embed democratic and participatory data governance and resource co-design with students and staff.

Equity data risks are fundamentally shared and collective, extending well beyond individual privacy to affect communities, cohorts, and cultures. Where governance decisions rely solely on internal risk classification, they are vulnerable to subjective judgement and poorly equipped to account for these collective dimensions of harm. Universities should recognise students and staff as co-governors of institutional data and digital technologies, formally embedding their participation in governance decision-making and oversight. In practice, this means ensuring meaningful student and staff membership on data governance committees and establishing standing co-design panels for the development and review of advanced

analytics systems and initiatives. Where equity impacts are significant, engagement should include First Nations representation and lived-experience expertise, including from disability and carer communities, informed by relevant Indigenous data governance frameworks and culturally safe practice. Universities should also actively work to develop and support senior leaders with lived experience of equity, including First Nations peoples and people with disability, ensuring that governance structures reflect and are accountable to the communities most affected by data practices.

8.4 Recommendations for senior university leaders, peak bodies, and professional associations

R8. Senior university leaders should ensure frontline equity support operates under a robust privacy-by-design data culture—backed by resourcing, clear policy, and safe escalation.

Frontline equity staff operate in a structural vulnerability where underdeveloped governance, unclear escalation pathways, and insufficient resourcing leave individuals exposed to professional risk and uncertain about how to raise concerns. Senior leaders should address this vulnerability directly by building a robust privacy-by-design data culture that supports and protects those working at the frontline of equity practice. This shift requires proactive attention across three areas.

First, culture and safety: Leaders should establish a culture of safe escalation, supported by clear non-retaliation policies and formal pathways for staff to report and escalate data concerns. Regular structured engagement with equity units would help ensure that operational realities remain visible to leadership, supporting ongoing improvement and providing direct acknowledgement of the ethical complexity staff navigate daily.

Second, systems and resourcing: Leaders should prioritise investment in modern digital infrastructure that supports the effective and ethical use of student data while mitigating its risks. This means ensuring teams have fit-for-purpose tools that embody privacy-by-design principles, enforce role-based access controls, and generate transparent and auditable records of data-handling decisions.

Third, clarity and accountability: Leaders should work with their teams to develop, document, and embed agreed data-handling procedures and clearly defined decision-making responsibilities. This formal clarity removes operational ambiguity, strengthens individual role accountability, and would help close the ethical grey zones that currently characterise day-to-day equity practice.

R9. Peak bodies and professional associations should co-design and publish field- and cohort-specific practice standards and exemplars for ethical equity data governance.

Significant work has already been done by professional associations, peak bodies, and community organisations to define ethical practice in relation to research involving equity cohorts. Frameworks such as the *CARE Principles for Indigenous Data Governance*,

alongside the longstanding call of “nothing about us without us”, reflect deep and sophisticated advocacy around data rights and participation. However, this work has not been consistently translated into the governance of internal university uses of student equity data—including evaluation, analytics, and operational data practices—where equivalent ethical obligations exist but formal guidance remains limited. Peak bodies, professional associations, and organisations representing equity cohorts and equity practitioners are well placed to extend and apply this existing expertise into the governance of internal university data practices. By co-designing and publishing field- and cohort-specific guidance that institutions can readily adopt or adapt, and by hosting open repositories of practice exemplars and accessible training, these bodies can support the translation of hard-won advocacy principles into the day-to-day governance of student data. This would provide direct practical support to frontline practitioners and support convergence towards national baselines.

This need will only grow. As national equity policy continues to evolve and new cohorts are formally recognised within equity frameworks, there is a strong case for ensuring that the communities most affected are meaningfully involved in shaping how their data is collected, used, and governed. The unique risks, vulnerabilities, and rights of each cohort cannot be assumed or extrapolated from existing frameworks; they must be understood on their own terms, in partnership with the communities themselves. Peak bodies and representative organisations are best placed to lead that work, and it falls to government and universities to ensure they are adequately resourced and supported to do so.

9. References

Anderson, P. J., & Diamond, Z. M. (2020). Stabilising and sustaining Indigenous leadership in Australian universities. In P. J. Anderson, K. Maeda, Z. M. Diamond, & C. Sato (Eds.), *Post-imperial perspectives on Indigenous education: Lessons from Japan and Australia* (pp. 186–208). Routledge. https://doi.org/10.4324/9780429400834

Andersson, S. (2023). Problems in information classification: Insights from practice. *Information & Computer Security*, *31*(4), 449–462. https://doi.org/10.1108/ICS-10-2022-0163

Anthony, D. L., & Stablein, T. (2016). Privacy in practice: Professional discourse about information control in health care. *Journal of Health Organization and Management*, *30*(2), 207–226. https://doi.org/10.1108/JHOM-12-2014-0220

Attorney-General's Department. (2022). *Privacy Act Review: Report 2022*. Australian Government. https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf

Australian Bureau of Statistics. (2020). Standard for sex, gender, variations of sex characteristics and sexual orientation variables. https://www.abs.gov.au/statistics/standards/standard-sex-gender-variations-sex-characteristics-and-sexual-orientation-variables/2020

Australian Government. (2023). *Government response – Privacy Act Review Report*. https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report

Australian Institute of Aboriginal and Torres Strait Islander Studies. (2020). *AIATSIS code of ethics for Aboriginal and Torres Strait Islander research*. https://aiatsis.gov.au/sites/default/files/2020-10/aiatsis-code-ethics.pdf

Australian Law Reform Commission. (2008). *For your information: Australian privacy law and practice* (Vol. 1, Report 108). https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol1.pdf

Australian National University. (2022, October 28). *Information and data classification (Standard).* Retrieved March 4, 2024.

Australian National University. (2022, October 28). *Data governance (Policy)*. Retrieved March 4, 2024.

Australian Pasifika Educators Network. (2023, April 30). *Response to the Australian Universities Accord Panel discussion paper [Submission to the Australian Universities Accord Panel].* https://www.education.gov.au/system/files/documents/submission-file/2023-05/Australian%20Pasifika%20Educators%20Network%20%28APEN%29.pdf

Baker, R. S., & Hawn, A. (2022). Algorithmic bias in education. *International Journal of Artificial Intelligence in Education*, *32*(4), 1052–1092. https://doi.org/10.1007/s40593-021-00285-9

Batchelor Institute of Indigenous Tertiary Education. (2016). *Privacy policy* (Policy No. SCS014, Version 2016-1).

Bonawitz, K., Wetmore, M., Heisler, M., Dalton, V. K., Damschroder, L. J., Forman, J., Allan, K. R., & Moniz, M. H. (2020). Champions in context: Which attributes matter for change efforts in healthcare? *Implementation Science*, *15*(1), Article 62. https://doi.org/10.1186/s13012-020-01024-9

Borgman, C. L. (2018). Open data, grey data, and stewardship: Universities at the privacy frontier. *Berkeley Technology Law Journal*, *33*(2), 365–412. https://doi.org/10.15779/Z38B56D489

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. Sage Publications.

Braunack-Mayer, A., Carolan, L., Street, J., Ha, T., Fabrianesi, B., & Carter, S. (2023). Ethical issues in big data: A qualitative study comparing responses in the health and higher education sectors. *PLOS ONE*, *18*(4), Article e0282285. https://doi.org/10.1371/journal.pone.0282285

Braunack-Mayer, A. J., Street, J. M., Tooher, R., Feng, X., & Scharling-Gamba, K. (2020). Student and staff perspectives on the use of big data in the tertiary education sector: A scoping review and reflection on the ethical issues. Review of Educational Research, 90(6), 788–823. https://doi.org/10.3102/0034654320960213

Brett, M. (2016). Disability and Australian higher education: Policy drivers for increasing participation. In A. Harvey, C. Burnheim, & M. Brett (Eds.), *Student equity in Australian higher education* (pp. 87–108). Springer Singapore. https://doi.org/10.1007/978-981-10-0315-8_6

Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). The CARE Principles for Indigenous Data Governance. *Data Science Journal*, *19*, Article 43. https://doi.org/10.5334/dsj-2020-043

CAST. (2024). *UDL Guidelines 3.0*. https://udlguidelines.cast.org

Cheong, P. H., & Nyaupane, P. (2022). Smart campus communication, internet of things, and data governance: Understanding student tensions and imaginaries. *Big Data & Society*, *9*(1). https://doi.org/10.1177/20539517221092656

Clark, C., Kusevskis-Hayes, R., & Wilkinson, M. (2019). How can universities encourage self-disclosure by equity students? *Journal of the Australian and New Zealand Student Services Association*, 27(1), 10–28. https://doi.org/10.30688/janzssa.2019.02

Corman, A., Canaway, R., Culnane, C., & Teague, V. (2022). Public comprehension of privacy protections applied to health data shared for research: An Australian cross-sectional study. *International Journal of Medical Informatics*, *167*, Article 104859. https://doi.org/10.1016/j.ijmedinf.2022.104859

Crawford, N. (2022). *"Equity" in higher education: What does this term mean and what are the practical implications for students in equity groups?* National Centre for Student Equity in Higher Education, Curtin University, Perth. https://www.ncsehe.edu.au/app/uploads/2022/06/StaffGuide-What-Is-Equity.pdf

Creswell, J. W., & Poth, C. N. (2024). *Qualitative inquiry and research design: Choosing among five approaches* (5th ed.). SAGE Publications, Inc.

Custers, B., & Vrabec, H. (2024). Tell me something new: Data subject rights applied to inferred data and profiles. *Computer Law & Security Review*, *52*, Article 105956. https://doi.org/10.1016/j.clsr.2024.105956

Department of Education. (2023). *Higher Education Provider* Guidelines 2023 (F2023L00400). Federal Register of Legislation. https://www.legislation.gov.au/F2023L00400/latest/text

Department of Education. (2024a). *Australian Universities Accord – Final report*. Australian Government. https://www.education.gov.au/australian-universities-accord/resources/final-report

Department of Education. (2024b). *Needs-based funding: Implementation consultation* (No. ESE24/1416-D24/3264935). Australian Government. https://www.education.gov.au/download/18360/needs-based-funding-implementation-consultation-paper/38323/document/pdf

Department of Employment, Education and Training. (1990). *A fair chance for all: National and institutional planning for equity in higher education. A discussion paper*. Australian Government Publishing.

Department of Industry, Science and Resources. (2024). *Safe and responsible AI in Australia: Proposals paper for introducing mandatory guardrails for AI in high-risk settings*. https://consult.industry.gov.au/ai-safety-and-guardrails/proposals-for-mandatory-guardrails-for-ai-in-high-risk-settings

Department of the Premier and Cabinet. (2020). *Premier and Cabinet Circular PC 012: Information Privacy Principles (IPPs) Instruction* (Cabinet Administrative Instruction No. 1 of 1989, amended 4 May 2020). Government of South Australia. https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf

Dollinger, M., & Lodge, J. (2019). What learning analytics can learn from students as partners. *Educational Media International*, *56*(3), 218–232. https://doi.org/10.1080/09523987.2019.1669883

Draper, N. A., Pieter Hoffmann, C., Lutz, C., Ranzini, G., & Turow, J. (2024). Privacy resignation, apathy, and cynicism: Introduction to a special theme. *Big Data & Society*, *11*(3). https://doi.org/10.1177/20539517241270663

Dreyfus, M. (2024, May 2). *Privacy by Design Awards 2024* [Speech]. https://www.markdreyfus.com/media/speeches/privacy-by-design-awards-2024-mark-dreyfus-kc-mp/

Fawns, T. (2023). Postdigital education. In P. Jandrić (Ed.), *Encyclopedia of postdigital science and education* (pp. 1–11). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-35469-4_52-1

Federation University. (2024, August 27). *Information Technology Services Operations Manual - Master Data Management, Data Classification and Usage, and Data Storage.* Retrieved Sept 3, 2024.

Flinders University. (2023, May 2). *Privacy policy*. Retrieved March 20, 2024.

Foster, J., McLeod, J., Nolin, J., & Greifeneder, E. (2018). Data work in context: Value, risks, and governance. *Journal of the Association for Information Science and Technology*, *69*(12), 1414–1427. https://doi.org/10.1002/asi.24105

Gale, T. (2012). Towards a southern theory of student equity in Australian higher education: Enlarging the rationale for expansion. *International Journal of Sociology of Education*, *1*(3), 238–262. https://doi.org/10.4471/rise.2012.14

Global Indigenous Data Alliance. (2023, January 23). *CARE principles for indigenous data governance*. https://www.gida-global.org/care

Grimes, S., Scevak, J., Southgate, E., & Buchanan, R. (2017). Non-disclosing students with disabilities or learning challenges: Characteristics and size of a hidden population. *The Australian Educational Researcher*, 44(4–5), 425–441. https://doi.org/10.1007/s13384-017-0242-y

Grimes, S., Southgate, E., Scevak, J., & Buchanan, R. (2019). University student perspectives on institutional non-disclosure of disability and learning challenges: Reasons for staying invisible. *International Journal of Inclusive Education, 23*(6), 639–655. https://doi.org/10.1080/13603116.2018.1442507

Harpur, P., Stafford, L., & Ellis, K. (2025). A disability-led disability inclusion strategy for the higher education sector. *Journal of Higher Education Policy and Management*, *47*(3), 368–385. https://doi.org/10.1080/1360080X.2025.2478537

Harvey, A., Burnheim, C., & Brett, M. (Eds.). (2016). *Student equity in Australian higher education*. Springer Singapore. https://doi.org/10.1007/978-981-10-0315-8

Harvey, A., Andrewartha, L., Sharp, M., & Wyatt-Smith, M. (2018). *Supporting younger military veterans to succeed in Australian higher education* [Report for the Australian Government Department of Veterans' Affairs]. Centre for Higher Education Equity and Diversity Research, La Trobe University. https://doi.org/10.26181/60efa14fb7067

Hayes, S., Jandrić, P., & Green, B. J. (2024). Towards a postdigital social contract for higher education in the age of artificial intelligence. *Postdigital Science and Education*, *6*(2), 467–485. https://doi.org/10.1007/s42438-024-00459-3

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2024). Inequalities in privacy cynicism: An intersectional analysis of agency constraints. *Big Data & Society*, *11*(1). https://doi.org/10.1177/20539517241232629

Hollinsworth, D., Raciti, M., & Carter, J. (2021). Indigenous students' identities in Australian higher education: Found, denied, and reinforced. *Race Ethnicity and Education*, 24(1), 112–131. https://doi.org/10.1080/13613324.2020.1753681

Jarke, J., & Büchner, S. (2024). Who cares about data? Data care arrangements in everyday organisational practice. *Information, Communication & Society*, *27*(4), 702–718. https://doi.org/10.1080/1369118X.2024.2320917

Jisc. (2024). *Data maturity framework*. https://beta.jisc.ac.uk/data-maturity-framework

Jisc. (2015). *Code of practice for learning analytics.* https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics

Kemp, K. (2023, March 31). *Ending the fictions in modern data practices: Submission in response to the Privacy Act Review Report* (SSRN Scholarly Paper No. 4521070). Social Science Research Network. https://doi.org/10.2139/ssrn.4521070

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148–152. https://doi.org/10.1145/1629175.1629210

Knight, S., Shibani, A., & Buckingham Shum, S. (2023). A reflective design case of practical micro-ethics in learning analytics. *British Journal of Educational Technology*, *54*(6), 1837–1857. https://doi.org/10.1111/bjet.13323

Komljenovic, J. (2021). The rise of education rentiers: Digital platforms, digital data and rents. *Learning, Media and Technology*, *46*(3), 320–332. https://doi.org/10.1080/17439884.2021.1891422

Komljenovic, J. (2022). The future of value in digitalised higher education: Why data privacy should not be our biggest concern. *Higher Education*, *83*(1), 119–135. https://doi.org/10.1007/s10734-020-00639-7

Komljenovic, J., Sellar, S., & Birch, K. (2024). Turning universities into data-driven organisations: Seven dimensions of change. *Higher Education*, *89*, 1369–1386. https://doi.org/10.1007/s10734-024-01277-z

Krebs, S., & Bennett, M. L. (2024). Data sharing agreements: Contracting personal information in the digital age. *Melbourne University Law Review*, *48*(1), 95–151. https://doi.org/10.3316/informit.T2024121100012390001183113

La Trobe University. (2023, August 17). *Privacy policy.* Retrieved March 3, 2024.

Li, W., Sun, K., Schaub, F., & Brooks, C. (2022). Disparities in students' propensity to consent to learning analytics. *International Journal of Artificial Intelligence in Education*, *32*(3), 564–608. https://doi.org/10.1007/s40593-021-00254-2

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry.* Sage Publications.

Liu, J. (2022). Social data governance: Towards a definition and model. *Big Data & Society*, *9*(2). https://doi.org/10.1177/20539517221111352

Liu, L. T., Wang, S., Britton, T., & Abebe, R. (2023). Reimagining the machine learning life cycle to improve educational outcomes of students. *Proceedings of the National Academy of Sciences*, 120(9). https://doi.org/10.1073/pnas.2204781120

Macfadyen, L. P., & Dawson, S. (2010). Mining LMS data to develop an "early warning system" for educators: A proof of concept. *Computers & Education*, *54*(2), 588–599. https://doi.org/10.1016/j.compedu.2009.09.008

McNamara, P., Harvey, A., & Andrewartha, L. (2019). Passports out of poverty: Raising access to higher education for care leavers in Australia. *Children and Youth Services Review, 97*, 85–93. https://doi.org/10.1016/j.childyouth.2017.07.015

Manwaring, K., Kemp, K., & Nicholls, R. (2021). *(Mis)informed consent in Australia*. UNSW Sydney. https://doi.org/10.26190/7SK3-0W49

Martin, L. (1994). *Equity and general performance indicators in higher education* (Vol. 1). Australian Government Publication Service.

Martin, L. (2016). Framing the framework: The origins of *A Fair Chance for All*. In A. Harvey, C. Burnheim, & M. Brett (Eds.), *Student equity in Australian Higher Education* (pp. 21–37). Springer Singapore. https://doi.org/10.1007/978-981-10-0315-8_2

McNicol, T., Carthouser, B., Bongiovanni, I., & Abeysooriya, S. (2024). Improving ethical usage of corporate data in higher education: Enhanced enterprise data ethics framework. *Information Technology & People*, *37*(6), 2247–2278. https://doi.org/10.1108/ITP-12-2022-0971

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1428

Molla, T. (2021). Refugees and equity policy in Australian higher education. *Policy Reviews in Higher Education*, *5*(1), 5–27. https://doi.org/10.1080/23322969.2020.1806727

Møller, N. H., Bossen, C., Pine, K. H., Nielsen, T. R., & Neff, G. (2020). Who does the work of data? *Interactions*, *27*(3), 52–55. https://doi.org/10.1145/3386389

Moses, L. B., & Weatherall, K. (2024). Data problems and legal solutions: Some thoughts beyond privacy. In *Data and the Digital Self: What the 21st century needs* (pp. 18–47). Australian Computer Society. https://www.acs.org.au/insightsandpublications/reports-publications/data-and-the-digital-self.html

Murdoch University. (2023, January 31). *Privacy policy*. Retrieved March 4, 2024.

National Health and Medical Research Council. (2023). *National statement on ethical conduct in human research 2023*. https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2023

Nguyen, H., & Cuong, L. (2025). Overview of data classification and applications in data security. *International Journal of Environmental Sciences*, *11*(13), 31–39. https://doi.org/10.64252/ac0b3685

Office of the Australian Information Commissioner. (n.d.-a). *Guide to developing an APP privacy policy*. Australian Government. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/guide-to-developing-an-app-privacy-policy

Office of the Australian Information Commissioner. (n.d.-b). *Tips for good privacy practice*. Australian Government. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/tips-for-good-privacy-practice

O'Shea, S., May, J., Stone, C., & Delahunty, J. (2024). *First-in-family students, university experience and family life: Motivations, transitions and participation*. Springer International Publishing. https://doi.org/10.1007/978-3-031-34451-0

Pangrazio, L. (2024). Data harms: The evidence against education data. *Postdigital Science and Education*, *6*(4), 1049–1054. https://doi.org/10.1007/s42438-024-00468-2

Pitman, T., Brett, M., & Ellis, K. (2023). Three decades of misrecognition: Defining people with disability in Australian higher education policy. *Disability & Society*, *38*(2), 323–341. https://doi.org/10.1080/09687599.2021.1937061

Popescu, M., Baruh, L., & Sudhakar, S. (2024). Role-based privacy cynicism and local privacy activism: How data stewards navigate privacy in higher education. *Big Data & Society*, *11*(2). https://doi.org/10.1177/20539517241240664

Prinsloo, P., Khalil, M., & Slade, S. (2024). Vulnerable student digital well-being in AI-powered educational decision support systems (AI-EDSS) in higher education. *British Journal of Educational Technology*, *55*(5), 2075–2092. https://doi.org/10.1111/bjet.13508

Prinsloo, P., & Slade, S. (2017). An elephant in the learning analytics room: The obligation to act. In *LAK '17: Proceedings of the Seventh International Learning Analytics & Knowledge Conference* (pp. 46–55). Association for Computing Machinery. https://doi.org/10.1145/3027385.3027406

Raaper, R., & Komljenovic, J. (2022). *The changing role of students in British higher education governance: Partners, consumers and digital users* (Working paper no. 79). Centre for Global Higher Education. https://ora.ox.ac.uk/objects/uuid:34a155a9-1c79-4f2e-a6b0-538bb0f4121e/files/rjh343t72g

Rana, V., & Azeez, G. K. (2025). Indigenous data sovereignty in Australian higher education: Paving the way for First Nations' self-determination. *Journal of Higher Education Policy and Management*, *47*(3), 426–434. https://doi.org/10.1080/1360080X.2025.2469920

Robinson, M., Tomaszewski, W., Kubler, M., Johnstone, M., Clague, D., Zajac, T., Povey, J., & Salom, C. (2021). *The Student Equity in Higher Education Evaluation Framework: Final report*. The Institute for Social Science Research, The University of Queensland. https://www.education.gov.au/heppp/resources/student-equity-higher-education-evaluation-framework-seheef-final-report

Rose, J., Langton, M., Smith, K., & Clinch, D. (2023). Indigenous data governance in Australia: Towards a national framework. *The International Indigenous Policy Journal*, *14*(1). https://doi.org/10.18584/iipj.2023.14.1.10987

Rule, J. B., & Greenleaf, G. W. (2010). *Global privacy protection: The first generation*. Edward Elgar Publishing.

Selvaratnam, R., Ames, K., & Leichtweis, S. (2024). *Governance of artificial intelligence and data in Australasian higher education: A snapshot of policy and practice* [White paper]. Australasian Council on Open, Distance and eLearning. https://doi.org/10.14742/apubs.2023.717

Shea, C. M. (2021). A conceptual model to guide research on the activities and effects of innovation champions. *Implementation Research and Practice*, *2*. https://doi.org/10.1177/2633489521990443

Sheridan, P. M. (2022). Edtech in higher education: Protecting student data privacy in the classroom. *North Carolina Journal of Law & Technology*, *21*(1), 49–84.

Sloane, M., Moss, E., Awomolo, O., & Forlano, L. (2022). Participation is not a design fix for machine learning. In *EAAMO '22: Proceedings of the 2nd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization* (pp. 1–6). Association for Computing Machinery. https://doi.org/10.1145/3551624.3555285

Soffer, T., & Cohen, A. (2024). Privacy versus pedagogy – students' perceptions of using learning analytics in higher education. *Australasian Journal of Educational Technology*, *40*(5), 14–30. https://doi.org/10.14742/ajet.9130

Solove, D. J. (2023). Data is what data does: Regulating based on harm and risk instead of sensitive data. *Northwestern University Law Review*, *118*(4), 1081–1138. https://heinonline.org/HOL/P?h=hein.journals/illlr118&i=1109

Solove, D. J. (2024). Murky consent: An approach to the fictions of consent in privacy law. *Boston University Law Review*, 104(2), 593–640. https://doi.org/10.2139/ssrn.4333743

Solove, D. J., & Hartzog, W. (2024). Kafka in the age of AI and the futility of privacy as control. *Boston University Law Review*, *104*, 1021–1042. https://scholarship.law.bu.edu/faculty_scholarship/3820

Sriprakash, A., Williamson, B., Facer, K., Pykett, J., & Valladares Celis, C. (2024). Sociodigital futures of education: Reparations, sovereignty, care, and democratisation. *Oxford Review of Education*, *51*(4), 561–578. https://doi.org/10.1080/03054985.2024.2348459

Stephenson, B., & Harvey, A. (2022). Student equity in the age of AI-enabled assessment: Towards a politics of inclusion. In R. Ajjawi, J. Tai, D. Boud, & T. Jorre De St Jorre (Eds.), *Assessment for inclusion in higher education: Promoting equity and social justice in assessment* (pp. 120–130). Routledge. https://doi.org/10.4324/9781003293101

Stephenson, B., Harvey, A., & Huang, Q. (2022). *Towards an inclusive analytics for Australian higher education*. National Centre for Student Equity in Higher Education, Curtin University, Perth. https://www.acses.edu.au/app/uploads/2022/03/Stephenson_LaTrobe_Final.pdf

Stone, M. A., Redsell, S. A., Ling, J. T., & Hay, A. D. (2005). Sharing patient data: Competing demands of privacy, trust and research in primary care. *British Journal of General Practice*, *55*, 783–789.

Swist, T., Buckingham Shum, S., & Gulson, K. N. (2024). Co-producing AIED ethics under lockdown: An empirical study of deliberative democracy in action. *International Journal of Artificial Intelligence in Education*, *34*(3), 670–705. https://doi.org/10.1007/s40593-023-00380-z

Taylor, M. J. (2020). "Personal information" and group data under the "Privacy Act 1988" (Cth). *Australian Law Journal*, *94*(10), 730–740. https://doi.org/10.3316/agispt.20201006037700

Tertiary Education Quality and Standards Agency. (2024). *Gen AI strategies for Australian higher education: Emerging practice*. Australian Government. https://www.teqsa.gov.au/guides-resources/resources/corporate-publications/gen-ai-strategies-australian-higher-education-emerging-practice

Tomaszewski, W., Kubler, M., Perales, F., Clague, D., Xiang, N., & Johnstone, M. (2020). *Investigating the effects of cumulative factors of disadvantage*. Institute for Social Science Research. https://espace.library.uq.edu.au/view/UQ:2a76ba9

Tomaszewski, W., Kubler, M., Perales, F., Western, M., Rampino, T., & Xiang, N. (2018). *Review of identified equity groups*. Institute for Social Science Research, The University of Queensland. https://espace.library.uq.edu.au/view/UQ:bd8a044

Tsai, Y.-S., Perrotta, C., & Gašević, D. (2020). Empowering learners with personalised learning approaches? Agency, equity and transparency in the context of learning analytics. *Assessment & Evaluation in Higher Education*, *45*(4), 554–567. https://doi.org/10.1080/02602938.2019.1676396

The University of Adelaide. (2017, July 17). *Privacy policy.* Retrieved February 22, 2024.

The University of Notre Dame Australia. (2024, April 9). *Procedure: Information management*. Retrieved May 1, 2024.

The University of Queensland. (2024, January 9). *Data handling procedure*. Retrieved April 20, 2024.

University of South Australia. (2021, February 12). *Privacy policy (Policy No. M-1).* Retrieved February 4, 2024.

The University of Western Australia. (2023, December 8). *Information privacy policy* (Policy No. UP14/10). Retrieved April 20, 2024.

University of Wollongong. (2023, December 21). *Support for Students Policy*. Retrieved May 10, 2024.

University of Wollongong. (2023, December 13*). Learning Analytics Data Use Policy*. Retrieved May 10, 2024.

van Toorn, G., & Scully, J. L. (2024). Unveiling algorithmic power: Exploring the impact of automated systems on disabled people's engagement with social services. *Disability & Society*, *39*(11), 3004–3029. https://doi.org/10.1080/09687599.2023.2233684

Viljoen, S. (2021). A relational theory of data governance. *The Yale Law Journal*, *131*, 573–654.

Walter, M., Lovett, R., Maher, B., Williamson, B., Prehn, J., Bodkin-Andrews, G., & Lee, V. (2021). Indigenous data sovereignty in the era of big data and open data. *Australian Journal of Social Issues*, *56*(2), 143–156. https://doi.org/10.1002/ajs4.141

Whitwell, S., & Clarke, S. (2023). Pedagogy of privacy: Inclusive teaching and disclosures of disability. In D. F. Quintel & A. York (Eds.), *Privacy and safety in online learning* (pp. 110–119). MTSU Pressbooks. https://mtsu.pressbooks.pub/privacyandsafetyinonlinelearning/chapter/pedagogy-of-privacy-inclusive-teaching-and-disclosures-of-disability/

Wong, W. H., Duncan, J., & Lake, D. A. (2024). Why data about people are so hard to govern. *Regulation & Governance*, *19*(1), 236–252. https://doi.org/10.1111/rego.12591

10. Appendices

10.1 List of Table A providers

The desktop institutional policy review, reported in Section 6 of this report, was limited to the following 39 Australian universities because they are designated as Table A providers under the *Higher Education Support Act 2003* (Cth, Compilation No. 92, January 2024):

Australian National University

Central Queensland University

Charles Darwin University

Charles Sturt University

Curtin University

Deakin University

Edith Cowan University

Federation University Australia

Flinders University

Griffith University

James Cook University

La Trobe University

Macquarie University

Monash University

Murdoch University

Queensland University of Technology

Royal Melbourne Institute of Technology

Southern Cross University

Swinburne University of Technology

The University of Adelaide

The University of Melbourne

The University of Notre Dame Australia

The University of Queensland

The University of Sydney

The University of Western Australia

University of Canberra

University of Newcastle

University of New England

University of New South Wales

University of South Australia

University of Southern Queensland

University of Tasmania

University of Technology Sydney

University of the Sunshine Coast

University of Wollongong

Victoria University

Western Sydney University

Australian Catholic University Limited

Batchelor Institute of Indigenous Tertiary Education

10.2 Interview guide

Semi-structured interview guide
Primary investigator: Dr Bret Stephenson
ACSES Equity Fellow, Australian Centre for Student Equity and Success
Data and Analytics, La Trobe University, Australia
[redacted]
Ph: [redacted]

This study has been approved by the La Trobe University Human Research Ethics Committee: ethics number HEC24361.

CENTRING STUDENT EQUITY IN DATA AND AI GOVERNANCE:
INFORMING POLICY TO EMPOWER PRACTICE

Please note: The following questions are intended as conversation prompts rather than fixed interview questions.

Initial comments

- Thank you very much for your time and for agreeing to participate in this study.
- Researcher self-introduction.
- Review of the study's protocol for protecting participant confidentiality and anonymity.
- Re-confirm the participant's full and voluntary consent to the interview.
- Do you have any questions before we start the interview?
- Do I have your permission to use the "live transcription" functionality of Teams to produce an initial draft transcription of the interview?
- Are you happy for me to start the recording?

Questions and discussion prompts

1. Can you please tell me about your role at (institution) and its relation to student equity (equity group) support efforts?

2. Can you tell me about how you utilise equity student data as part of your role?

3. What challenges have you encountered in relation to accessing, utilising, and sharing equity student data?

4. What are some key considerations or challenges that you have encountered for maintaining the privacy of equity student information? Is this a concern?

5. Are you familiar with your institution's policies and procedures relating to student data (or information) governance and privacy?

    a. Are these well socialised?

6. Do you believe that your institution's policies and procedures are effective, and effectively implemented, towards managing the potential risks associated with the collection and use of personal student equity data?

    a. For example, is it clear who should be given access to student equity data and for what purposes? Is it clear how, and by whom, these decisions are made?
    b. How could these policies and procedures be improved?

7. Are there opportunities for (greater) student participation in data governance or use decisions, or opportunity to give students greater control over their data?

    a. Would this be desirable?
    b. Are there technological or organisational barriers to this?

8. Can you offer any examples of how digital technologies—*learning analytics*, *predictive analytics*, or *artificial intelligence*—are being used to support the success and wellbeing of equity students?

    a. Does your institution have specific policies, procedures, or guidelines relating to the use of these technologies? (For example, ethics guidelines)
    b. Do these policies or strategy documents address specific equity concerns or goals?

9. Is there anything else that you would like to add in relation to improving the way universities responsibly collect, manage, and utilise student equity data?

End recording