The HiVE - Acceptable Use Policy

Version 1.0 - Effective from August 2017

This Acceptable Use Policy (the "Policy") describes prohibited uses and activities in respect of the services ("Services") provided by Harvest Digital Planning Pty Ltd (ABN 53 102 443 916) ("we", "us" or "our") for access to and use of our The HiVE Digital Engagement System (including any apps, databases, platforms, networks, websites and APIs) and any other related services. This Policy is incorporated by reference into The HiVE - Terms of Service ("Terms").

All users of the Services (including Authorised Users and End Users) are required to comply with this Policy at all times.

1. Prohibited uses

In using our Services, you agree not to misuse them and are prohibited from engaging in any of the following activities:

1. unlawful activities;
2. publishing or sharing any material that:
    a. breach any applicable law, standard, code or other legislative or regulatory requirement including, without limitation, storing, publishing or sharing any material that is fraudulent, defamatory, or misleading;
    b. infringes or misappropriates the intellectual property or proprietary rights of any other person;
    c. is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes pornography or extreme acts of violence;
    d. advocates bigotry or hatred against any person or group of people based on their race, religion, ethnicity, sex, gender identity, sexual preference, disability or impairment; or
    e. is intended to be inflammatory;
3. uploading or otherwise disseminating viruses, adware, spyware, worms, or other malicious code that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots;
4. violating the privacy or infringing the rights of any other person;

5. probing, scanning, or testing the vulnerability of any system or network;
6. breaching or otherwise circumventing any security or authentication measures;
7. accessing, tampering with, or using non-public areas or parts of the Services, or shared areas of the Services you haven't been invited to;
8. disabling, interfering with or circumventing any other aspect of the Services;
9. monitoring data, traffic or other activities undertaken in connection with the Services without permission;
10. making network connections to any users, hosts, or networks unless you have permission to communicate with them;
11. operating network services like open proxies, open mail relays, or open recursive domain name servers;
12. accessing, searching, or creating accounts for the Service by any means other than our publicly supported interfaces (for example, "scraping" or creating accounts in bulk);
13. sending unsolicited communications, promotions or advertisements, or spam;
14. sending altered, deceptive or false source-identifying information, including "spoofing" or "phishing";
15. using manual or electronic means to avoid any use limitations placed on the Services, such as access and storage restrictions;
16. accessing or using the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas;
17. developing or creating a competing service or product;
18. copying, modifying, creating a derivative work of, reverse engineering, decompiling, translating, disassembling, or otherwise attempting to extract the source code of the Services or any component of the Services;
19. providing access to anyone who is not an authorised user;
20. sub-licensing, reselling, or distributing the Services or any component thereof separate from any integrated application;
21. going far beyond the use parameters for any given service or feature as described in any corresponding documentation or advice from us;
22. using the Services to stalk, harass, or post direct, specific threats of violence against others; or
23. engaging in any activity that adversely affects, or may adversely affect, our reputation or goodwill or the reputation or goodwill of any third party.

Please note this list is not exhaustive and is meant to represent the types of activities that are prohibited.

2. Breaches of this Policy

If you breach this Policy or authorise or help others to do so, we may suspend or terminate your use of the Services in accordance with the Terms. If you use the Services under an employer or organization's account, we reserve the right to notify your employer or organization of any actual or suspected breach of this Policy.

If you become aware of any breach of this Policy, you must immediately notify us and provide us with assistance, as requested, to stop or remedy the breach.

To report any breach of this Policy, please email us at *support@harvestdp.com*.

We reserve full and final discretion as to whether any use of the Services breach this Policy. By using the Service, you agree that our determination as to whether any use of the Services breach this Policy is final.

3. Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any breach of this Policy (including, without limitation, any misuse of the Services). In doing so, we may:

(i) remove, disable access to, or modify any content or resource that we consider breaches this Policy, the Terms or any other agreement we have with you for use of the Services; and

(ii) report to appropriate law enforcement officials, regulators or other appropriate third parties any activity that we suspect breaches any law, standard, code or other legislative or regulatory requirement.

4. Changes to this Policy

We reserve the right to modify this Policy from time to time, in our sole discretion, and the modified Policy shall be effective thirty (30) days after you have been notified that it has been posted on our website at www.the-hive.com. You acknowledge and agree that you are responsible for reviewing the most recent version of this Policy which has been posted on our website.