Information Security Policy

1. INTRODUCTION

1.1. Hyve is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

1.2. In relation to personal information, under Retained Regulation (EU) 2016/679, UK General Data Protection Regulation (UK GDPR), Hyve must:

(i) use technical or organisational measures to ensure personal information is kept secure, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage;

(ii) implement appropriate technical and organisational measures to demonstrate that it has considered and integrated data compliance measures into Hyve's data processing activities; and

(iii) be able to demonstrate that it has used or implemented such measures.

1.3. The purpose of this policy is to:

(i) protect against potential breaches of confidentiality;

(ii) ensure all our information assets and its facilities are protected against damage, loss or misuse;

(iii) support Hyve's data protection policy in ensuring all staff are aware of and comply with UK law and Hyve's procedures applying to the processing of personal information; and

(iv) increase awareness and understanding in Hyve of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

2. DEFINITIONS

Business Information shall mean business-related information other than personal information regarding customers, clients, suppliers and other business contacts of Hyve;

Confidential Information shall mean trade secrets or other confidential information (either belonging to Hyve or to third parties) that is processed by Hyve;

Personal Information (sometimes known as personal data) shall mean information relating to an individual who can be identified (directly or indirectly) from that information;

Pseudonymised shall mean the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

Sensitive Personal Information (sometimes known as 'special categories of personal data', 'special category data' or 'sensitive personal data') shall mean personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3. ROLES AND RESPONSIBILITIES

3.1. Information security is the responsibility of all staff. The Legal and Compliance Departments are, in particular, responsible for:

(i) monitoring and implementing this policy;

(ii) monitoring potential and actual security breaches;

(iii) ensuring that staff are aware of their responsibilities; and

(iv) ensuring compliance with the requirements of retained regulation (EU) 2016/679 UK GDPR and other relevant legislation and guidance.

4. SCOPE

4.1. The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of Hyve, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

4.2. This policy applies to all staff, including employees, temporary and agency workers, other contractors, interns, volunteers and apprentices.

4.3. All staff must be familiar with this policy and comply with its terms.

4.4. Hyve information covered by this policy may include:

(i) personal information relating to staff, customers, clients, suppliers;

(ii) other business information; and

(iii) confidential information.

4.5. This policy supplements Hyve's Data Protection Policy- Employment and other policies and privacy notices relating to Data Protection and Records Retention and the contents of those policies must be taken into account, as well as this policy.

4.6. We will review and update this policy regularly in accordance with our data protection and other obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy when it is adopted.

5. GENERAL PRINCIPLES

5.1. All Hyve information must be treated as commercially valuable and protected from loss, theft, misuse or inappropriate access or disclosure.

5.2. Personal Information, and Sensitive Personal Information, must be protected against unauthorised and/or unlawful processing and against accidental loss, destruction or damage, by the use of appropriate technical and organisational measures.

5.3. Staff should discuss with department managers the appropriate security arrangements and technical and organisational measures which are appropriate and in place for the type of information they access in the course of their work.

5.4. Hyve Information (other than Personal Information) is owned by Hyve and not by any individual or department.

5.5. Hyve information must be used only in connection with work being carried out for Hyve and not for other commercial or personal purposes.

5.6. Personal Information must be used only for the specified, explicit and legitimate purposes for which it is collected.

6. INFORMATION MANAGEMENT

6.1. Personal Information must be processed in accordance with:

(i) the data protection principles, set out in Hyve's Data Protection Policy;

(ii) Hyve's Data Protection Policy generally; and

(iii) all other relevant policies.

6.2. In addition, all information collected, used and stored by Hyve must be:

(i) adequate, relevant and limited to what is necessary for the relevant purposes;

(ii) kept accurate and up to date.

6.3. Hyve will take appropriate technical and organisational measures to ensure that Personal Information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage, including:

(i) Pseudonymisation of Personal Information;

(ii) Encryption of Personal Information.

6.4. Personal Information and Confidential Information will be kept for no longer than is necessary and stored and destroyed in accordance with Hyve's Records Retention Policy.

7. HUMAN RESOURSES INFORMATION

7.1. Given the internal confidentiality of personal files, access to such information is limited to the HR department. Except as provided in individual roles, other staff are not authorised to access that information.

7.2. Any staff member in a management or supervisory role or involved in recruitment must keep personnel information strictly confidential.

7.3. Staff may ask to see their personnel files and any other Personal Information in accordance with Retained Regulation (EU) 2016/679, UK GDPR and other relevant legislation. For further information, see Hyve's Data Subject Access Request Policy.

8. ACCESS TO OFFICES AND INFORMATION

8.1. Office doors, keys and fobs must be kept secure at all times and keys or fobs must not be given to any third party at any time.

8.2. Documents containing Confidential Information and equipment displaying Confidential Information should be positioned in a way to avoid them being viewed by people passing by, eg through office windows.

8.3. Visitors must be required to sign in at reception, accompanied at all times and never left alone in areas where they could have access to Confidential Information.

8.4. Wherever possible, visitors should be seen in meeting rooms.

8.5. At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing Confidential Information must be securely locked away.

9. **COMPUTERS AND IT**

9.1. Password protection and encryption must be use where available on Hyve systems in order to maintain confidentiality.

9.2. Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords must not be written down or given to others.

9.3. Computers and other electronic devices must be locked when not in use and when you leave your desk, to minimise the risk of accidental loss or disclosure.

9.4. Confidential Information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/thumb drive without the express permission of the Tech or Support departments.

9.5. All electronic data must be securely backed up at the end of each working day. This happens automatically for all data stored on Hyve's computer network.

9.6. Staff must ensure they do not introduce viruses or malicious code on to Hyve systems. Software must not be installed or downloaded from the internet without it first being virus checked. Staff should contact Tech or Support for guidance on appropriate steps to be taken to ensure compliance.

10. **COMMUNICATION AND TRANSFER OF INFORMATION**

10.1. Staff must be careful about maintaining confidentiality when speaking in public places, eg when speaking on a mobile telephone.

10.2. Confidential Information must be marked 'private and confidential' and circulated only to those who need to know the information in the course of their work for Hyve. Further details of how emailed information must be marked and protected are set out in Hyve's Records Management Policy, IT, Email and Communications Policy and in the rest of this section of the policy.

10.3. Confidential Information must not be removed from Hyve's offices unless required for authorised business purposes, and then only in accordance with paragraph 10.4 below.

10.4. Where Confidential Information is permitted to be removed from Hyve's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that Confidential Information is:

(i) Stored on an encrypted device with strong password protection, which is kept locked when not in use;

(ii) When in paper copy, not transported in see-through or other unsecured bags or cases;

(iii) Not read in public places (eg waiting rooms, cafes, trains); and

(iv) Not left unattended or in any place where it is at risk (eg in conference rooms, car boots, cafes).

10.5. Postal, document exchange (DX) and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

10.6. All Sensitive Information or particularly Confidential Information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

11. **PERSONAL EMAIL AND CLOUD STORAGE ACCOUNTS**

11.1. Personal email accounts, such as yahoo, google or Hotmail and cloud storage services, such as dropbox, icloud and onedrive are vulnerable to hacking. They do not provide the same level of security as the services provided by our own IT systems.

11.2. Do not use a personal email account or cloud storage account for work purposes.

11.3. If you need to transfer a large amount of data, contact Tech or Support for help.

12. **HOME WORKING**

12.1. Staff must not take Hyve information home unless required for authorised business purposes, and then only in accordance with paragraph 12.2 below.

12.2. Where staff are permitted to take Hyve information home, staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular:

(i) Personal and Confidential Information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

(ii) all Personal and Confidential Information must be retained and disposed of in accordance with paragraph 6.4 above.

12.3. Staff must not store Confidential Information on their home computers (PCs, laptops or tablets).

12.4. You should refer to Hyve's Homeworking Policy for further information.

13. **TRANSFER TO THIRD PARTIES**

13.1. Third parties should be used to process Hyve information only in circumstances where appropriate written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings. Consideration must be given to whether the third parties will be processors for the purposes of Retained Regulation (EU) 2016/679, UK GDPR.

13.2. Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult Legal at legal@hyve.com or Compliance at compliance@hyve.com.

14. **OVERSEAS TRANSFER**

14.1. There are restrictions on international transfers of Personal Information and transfers to international organisations. Staff must not transfer Personal Information outside the UK or to international organisations.

14.2. You should refer to Hyve's Data Protection Policy for further information on international transfers.

15. **TRAINING**

15.1. All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided whenever there is a substantial change in the law or our policy and procedure.

15.2. Compliance and Legal will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or our information management and security policy or procedures, please contact Legal or Compliance.

16. **REPORTING BREACHES**

16.1. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows Hyve to:

(i) Investigate the failure and take remedial steps if necessary;

(ii) Maintain a register of compliance failures; and

(iii) Make any applicable notifications.

16.2. Please refer to our Personal Data Breach Plan for our reporting procedure.

17. **CONSEQUENCES OF FAILING TO COMPLY WITH THIS POLICY**

17.1. Hyve takes compliance with this policy very seriously. Failure to comply with it puts both staff and Hyve at significant risk. The importance of this policy means that failure to comply with any requirement of it may lead to disciplinary action, which may result in dismissal.

17.2. Staff with any questions or concerns about anything in this policy should not hesitate to contact Legal at legal@hyve.com or Compliance at compliance@hyve.com.

18. **DOCUMENT HISTORY**

Revision Date	Version no.	Amendment	Authorised by:	New Version No.
7th September 2022	1.1	Created by Briona Gander	Jamie Todd	1.2