Haven (Tyneside) Ltd

Data Protection and Retention Policy and Guidance

Policy Profile	
Implementation Date	January 2019
Last Review Date	January 2019
Next Review Date	January 2020
Version	3

Approval Record	
Policy Owner	Chief Officer

Data Protection and Retention Policy

1. EXECUTIVE SUMMARY

1.1 This policy should be read and understood by Haven (Tyneside) Limited's ("we,", "our", "us", "the Company") employees, trustees, officers, agency workers, other workers and volunteers.

1.2 The policy sets out what processes are in place to ensure that personal data (as defined in section 22) is obtained, handled, stored and destroyed in accordance with GDPR. It explains what is required of our staff (which, for the purposes of this policy, shall include agency workers and other contractors) to enable us to comply with applicable law.

1.3 All personal data must be processed (as defined in section 22) in accordance with the data protection principles. In particular:

1.3.1 You must have a lawful basis for processing personal data (for more information see section 6);

1.3.2 Once you have collected personal data for a particular purpose, it must only be used for that purpose (for more information please see section 7);

1.3.3 You cannot collect and process personal data unless it required as part of your job (for more information please see section 8);

1.3.4 You must ensure that personal data is accurate and is kept up to date (for more information please see section 9);

1.3.5 You should not keep personal data for longer than is reasonably necessary (for more information please see section 10);

1.3.6 You must comply with requirements to ensure the security, integrity and confidentiality of personal data (for more information please see section 11);

1.3.7 You should not transfer personal data outside the EEA without first contacting the Chief Officer or Operations Manager (for more information please see section 12);

1.3.8 Data subjects have certain rights in relation to their personal data (for more information please see section 13).

1.4 You should exercise particular caution when undertaking direct marketing or sharing personal data (please see sections 17 and 18 for more information).

1.5 Data should not be kept indefinitely. Some 'disposable' data can be deleted once it has served its useful purpose, whilst other, more formal data should be kept and then destroyed in accordance with our data retention periods (please see section 19 and Appendix 1 for further information).

1.6 You will be asked to undertake regular training in relation to data protection and data privacy. For more information please see section 15.

1.7 If you have any queries, or need to report a data breach, please contact the Chief Officer or Operations Manager. For more information see section 4.

1.8 This document does not form part of employees' contracts of employment. Haven reserves the right to amend, update and/or replace this document from time to time.

1.9 Compliance with this document is of utmost importance to Haven. Breaches by employees may lead to disciplinary action, which could include summary dismissal for gross misconduct.

2. PURPOSE

2.1 In order to operate and carry out its charitable work, Haven needs to collect, use and retain certain types of information about the people with whom it comes into contact. These include current, past and prospective employees, clients and service users, suppliers, trustees and others with whom it communicates (who are all, Data Subjects). We take the issue of data protection very seriously and regard the lawful and correct treatment of personal data with the utmost importance to guarantee the successful operation of Haven and to maintain the confidence of those with whom we come into contact.

2.2 This policy therefore sets out how we handle the personal data of Data Subjects. The Policy also explains our requirements to retain data and to dispose of data and provides guidance (at Appendix 1) on appropriate data handling and disposal.

2.3 In the course of their employment with Haven, our staff will have contact with a variety of confidential and sensitive personal data belonging to a range of Data Subjects.

2.4 The Policy and guidelines listed below are of critical importance and non-compliance could in certain circumstances constitute a serious disciplinary matter. It is an internal document, although we may decide or be required to publish or otherwise share this policy.

3. SCOPE

3.1 Personal data must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer or recorded on any other material/within any form of

media. A number of safeguards to ensure this are set out in the GDPR (as implemented in the UK). In addition, the GDPR sets out powers to fine organisations for most serious breaches of GDPR up to the greater of €20million or 4% of annual worldwide turnover. Haven fully endorses and adheres to the GDPR and the data protection principles set out in the Data Protection Act 2018. We have therefore put in place working practices and procedures to ensure compliance with our legal obligations.

3.2 We are required to ensure that all personal data held by us is retained and destroyed securely. Compliance with the contents of this policy will help ensure compliance with our legal obligations.

3.3 This Policy applies to physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also applies to electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings.

3.4 A number of words and phrases that have a particular meaning in this policy are defined in section 22.

3.5 **Processing**

3.5.1 You will process personal data when you obtain, record, read, hold or use personal data.

3.5.2 All of the following activities will constitute the processing of personal data (without limitation):

(a) obtaining, filing, collecting, recording, organising, structuring or storing data;

(b) adapting or altering data;

(c) retrieving, consulting or using data;

(d) consulting with someone on the content of data or otherwise using it;

(e) disclosing data by transmitting it, disseminating it or otherwise making it available (including disclosures made to other employees or clients);

(f) combining the data with other data or aligning data; and

(g) restricting, erasing or destroying data.

4. ROLES AND RESPONSIBILITIES

4.1 It is the duty of all of our staff to ensure that they are fully aware of this policy and that they comply with its instructions.

4.2 Any queries relating to the contents of this Policy should be referred to the Chief Officer or Operations Manager. In addition, you should always contact the Chief Officer or Operations Manager in the following circumstances:

4.2.1 if you are unsure of the lawful basis which you are relying on to process personal data (including, if relying on legitimate interests, what those legitimate interests are);

4.2.2 if you need to rely on consent (as defined in section 22 below) and/or explicit consent in order to process personal data;

4.2.3 if you need to draft privacy notices (as defined in section 22) – i.e. notices to Data Subjects telling them how you will use their data;

4.2.4 if you are unsure about the retention period for the personal data being processed;

4.2.5 if you are unsure about what security or other measures you should follow to protect personal data;

4.2.6 if there has been a personal data breach (as defined in section 22);

4.2.7 if you are unsure whether you are able to transfer personal data outside the EEA;

4.2.8 if you need any assistance dealing with any rights invoked by a Data Subject;

4.2.9 whenever you are engaging in a significant new, or change in, processing activity which is likely to require a data privacy impact assessment (DPIA) (as defined in section 22) or if you plan to use personal data for purposes other than those for which it was collected;

4.2.10 if you plan to undertake any activities involving automated processing including profiling or automated decision-making (as defined in section 22);

4.2.11 if you need help complying with applicable law when carrying out direct marketing activities; or

4.2.12 if you need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors).

5. PERSONAL DATA PROTECTION PRINCIPLES

5.1 Personal data must be processed in accordance with seven enforceable principles to which all staff must make all reasonable efforts to adhere. The principles state that personal data must be:

5.1.1 processed fairly, lawfully and in a transparent manner (Lawfulness, Fairness and Transparency);

5.1.2 collected only for specified, explicit and legitimate purposes (Purpose Limitation);

5.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation);

5.1.4 accurate and where necessary kept up to date (Accuracy);

5.1.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation);

5.1.6 processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

5.1.7 not transferred to another country without appropriate safeguards in place (Transfer Limitation); and

5.1.8 made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their personal data (*Data Subject's Rights and Requests*).

5.2 More information is provided about each of these principles in the following sections.

5.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above, as well as ensuring we have adequate resources and controls in place to ensure and document GDPR compliance.

6. LAWFULNESS, FAIRNESS AND TRANSPARENCY

6.1 Lawfulness

6.1.1 You may only collect, process and share personal data fairly and lawfully and for specified purposes. In order to be lawful, processing personal data must meet at least one of the following conditions:

(a) the Data Subject has given his or her consent (please see below* on how consent is given);

(b) the processing is necessary for the performance of a contract with the Data Subject (e.g. where we have entered into a contract with an individual to provide them with particular services);

(c) the processing is necessary to meet our legal obligations (i.e. a common law or statutory obligation, rather than a contractual obligation);

(d) the processing is necessary to protect someone's vital interests (i.e. a life or death situation);

(e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller (as defined in section 22 below) (i.e. if we have a basis in law for exercising official authority or carrying out tasks in the public interest);or

(f) the processing is necessary to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

6.1.2 It is important that you identify and record the legal ground being relied on for each processing activity and where consent is relied on, evidence of that consent is recorded. Where data is collected under the remit of a privacy notice, this should explain the legal ground(s) being relied on for processing that personal data.

6.1.3 *A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing and the purposes for it. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

6.1.4 Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly actioned so that those Data Subjects are no longer contacted. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.2 **Special Category and Criminal Convictions Data**

6.2.1 Special category data and criminal convictions data (as defined in section 22 below) is more sensitive in nature, so needs more protection.

6.2.2 For special categories of personal data, in addition to having one or more of the lawful bases set out above, you will also need to satisfy one of the following specific conditions for processing:

(a) the Data Subject has given explicit consent (as defined in section 22 below);

(b) the processing is necessary for the purposes of employment, social security or social protection law;

(c) the processing is necessary to protect someone's vital interests where the Data Subject is incapable of giving consent;

(d) the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim and processing relates to members or former members in connection with the body's purposes;

(e) the processing is manifestly made public by the Data Subject;

(f) the processing is necessary for legal claims;

(g) the processing is necessary for reasons of substantial public interest;

(h) the processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health and social care systems and services;

(i) the processing is necessary for public health; or

(j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguarding.

6.2.3 For processing criminal conviction data, in addition to having one or more of the lawful bases set out above, you must either have 'official authority' or 'legal authority' for the processing. 'Official authority' is where the data is being processed in an official capacity. 'Legal authority' is where:

(a) the Data Subject has consented to the processing;

(b) the processing is necessary for the purposes of employment, social security or social protection law;

(c) the processing is necessary to protect someone's vital interests where the Data Subject is incapable of giving consent;

(d) the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim and processing relates to members or former members in connection with the body's purposes;

(e) the processing is manifestly made public by the Data Subject;

(f) the processing is necessary for legal claims;

(g) the processing is necessary for reasons of substantial public interest;

6.2.4 Where you are processing special categories of personal data or criminal conviction data, the condition(s) you are relying on must also be recorded in the relevant privacy notice.

6.3 **Fairness**

You must use personal data in a way that is fair. This means you must not process the personal data in a way that is unduly detrimental, unexpected or misleading to the data subject. You should only process personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. This will therefore depend in part on the purposes for which the personal data was obtained.

6.4 **Transparency**

6.4.1 Transparent processing is about being clear, open and honest with Data Subjects and how and why their personal data will be processed.

6.4.2 The GDPR requires Controllers to provide detailed, specific information to Data Subjects through appropriate privacy notices, explaining how the information was collected from them (including whether directly from Data Subjects or from elsewhere).

6.4.3 Where we collect personal data directly from Data Subjects (including for human resources or employment purposes), we therefore need to provide the Data Subject with this information in a privacy notice.

6.4.4 When personal data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting or receiving the data, through a privacy notice. We must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

7. **PURPOSE LIMITATION**

Personal data must be collected only for specified, explicit and legitimate purposes. Once collected for these purposes, it must not be processed in any manner incompatible with those purposes. You therefore must not use personal data for new, different or incompatible purposes to those purposes for which it was first obtained unless you have informed the Data Subject of

the new purposes and they have consented where necessary (i.e. where consent is relied on as the legal basis for processing).

8. DATA MINIMISATION

8.1 You may only process personal data obtained by us or on our behalf when required in performance of your duties as a member of our staff. You cannot process personal data for any reason unrelated to the duties of your job.

8.2 You should therefore only collect personal data that you require for your job and avoid collecting excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

8.3 You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines.

9. ACCURACY

We must together ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must ensure the accuracy of any personal data at the point of collection and our central mechanism for monitoring personal data will monitor the accuracy of personal data on an ongoing basis, although you should also destroy or amend any personal data you know to be inaccurate. You must take all reasonable steps to securely destroy or amend inaccurate or out-of-date personal data.

10. STORAGE LIMITATION

10.1 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our organisation operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our organisation.

10.2 You must not keep personal data in a form which permits the identification of the Data Subject for longer than needed for the purpose(s) for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.3 The retention procedures set out below help to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

10.4 You must take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with section 19 and Appendix 2. This includes requiring third parties to delete that data where applicable.

10.5 You must ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

11. SECURITY, INTEGRITY AND CONFIDENTIALITY

11.1 You must not send personal data relating to clients/residents, potential clients/residents, or former clients/residents by email under any circumstances.

11.2 We will develop, implement and maintain appropriate safeguards (such as anti-virus software and firewalls) and will evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are collectively responsible for protecting the personal data we hold (for example by not sending it to third parties without a lawful basis for doing so).

11.3 You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data (this is particularly important where you taking personal data outside of the office or personal data is accessible through a portable device, such as a work mobile phone). You must exercise particular care in protecting special categories of personal data and criminal convictions data from loss and unauthorised access, use or disclosure, because of the particularly sensitive nature of this information.

11.4 You must follow all procedures we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

11.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

11.6 The personal data you process in the course of your employment must not be disclosed to any person or other employees or outside the organisation otherwise than in the proper performance of your duties during your employment by the organisation.

12. TRANSFER LIMITATION

12.1 The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

12.2 You may only transfer personal data outside the EEA if certain conditions apply. If you are engaged in any activity that means you are likely to transfer personal data outside the EEA, please contact the Chief Officer or Operations Manager, who will be able to advise you on whether the transfer is permitted.

13. **DATA SUBJECT'S RIGHTS AND REQUESTS**

13.1 Data Subjects have rights when it comes to how we handle their personal data. These include rights to:

13.1.1 withdraw consent to processing at any time;

13.1.2 receive certain information about the Controller's processing activities;

13.1.3 request access to their personal data that we hold;

13.1.4 prevent our use of their personal data for direct marketing purposes;

13.1.5 ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

13.1.6 challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

13.1.7 request a copy of an agreement under which personal data is transferred outside of the EEA;

13.1.8 object to decisions based solely on automated processing, including profiling;

13.1.9 prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

13.1.10 be notified of a personal data breach which is likely to result in high risk to their rights and freedoms; and

13.1.11 in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

13.2 A Data Subject may contact you to exercise one or more of these rights over the data we hold about them. You must verify the identity of an individual requesting data under any of the rights listed above (third parties may only make requests on behalf of a Data Subject with proper authorisation).

13.3 If you receive a Data Subject request you should forward this immediately to your line manager.

14. **RECORD KEEPING**

14.1 The GDPR requires us to keep full and accurate records of all our data processing activities.

14.2 You must keep and maintain accurate records reflecting your processing of personal data including records of consent given by Data Subjects, the procedures for obtaining consents and purposes for which consent has been given.

15. TRAINING AND AUDIT

15.1 We are required to ensure all our staff have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance. You must therefore complete all mandatory data privacy related training and ensure that those members of your team for whom you are responsible undergo similar mandatory training.

15.2 You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

16. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

16.1 'Privacy by design' means data protection that is built into to an organisation's processing activities and business practices, so that data protection and privacy issues are considered upfront in the way technical and organisational matters are designed and implemented (for example, by adopting systems that minimise the processing of personal data, and enabling people to monitor the processing).

16.2 We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

16.3 You must assess what privacy by design measures can be implemented on all programmes, systems or processes that you use or are responsible for that process personal data by taking into account the following:

16.3.1 the normal standards and best practice;

16.3.2 the cost of implementing any measures;

16.3.3 the nature, scope, context and purposes of processing; and

16.3.4 the risks that your processing poses to the rights and freedoms of Data Subjects (for example, if your processing creates a high risk that a Data Subject's rights will be impacted in some way, it is more important to consider and implement privacy by design).

17. DIRECT MARKETING

17.1 We are subject to certain rules and privacy laws when marketing to our customers, donors, service users and stakeholders.

17.2 For example, a Data Subject's prior express Consent is required for electronic direct marketing (for example, by email, text or automated calls).

17.3 If we engage in direct marketing, the right to object to direct marketing must be explicitly offered to the Data Subject in a clear and understandable manner so that it is clearly distinguishable from other information.

17.4 A Data Subject's objection to direct marketing must be promptly honoured and recorded.

18. SHARING PERSONAL DATA

18.1 Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

18.2 You may only share the personal data we hold with another member of staff if the recipient has a job-related need to know the information (if sharing is happening as part of work-related activity, this is likely to be met).

18.3 You may only share the personal data we hold with third parties, such as our service providers or partners, if:

18.3.1 they have a need to know the information for the purposes of providing the contracted services;

18.3.2 sharing the personal data complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;

18.3.3 the third party has put adequate security measures in place and agreed to comply with the required data security standards, policies and procedures (including compliance with GDPR and agreement not to send any personal data relating to our clients by email);

18.3.4 the transfer complies with any applicable cross-border transfer restrictions; and

18.3.5 a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

18.4 Please contact the Chief Officer or Operations Manager if you need to find out whether a proposed transfer to a third party meets with these requirements.

19. DATA RETENTION

19.1 The principles of data minimisation and storage limitation (set out above) apply when considering retention of personal data.

19.2 The Operations Manager is responsible for identifying the data that we must or should retain, and determining the proper period of retention (seeking advice where required to do so). This person is also responsible for administering data management programmes and providing guidance to our staff on data retention and disposal.

19.3 **Data classifications**

19.3.1 Certain data, including formal or official records, is more important to us and is therefore listed in the record retention schedule (set out in Appendix 2). This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our organisation. Some of this information may also be confidential and should be afforded with the appropriate degree of security, including restricting who within and outside the Company is permitted access to it (for example, password protecting data relating to criminal histories of service users). Any confidential information that an employee may have obtained from a source outside of the Company, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us.

19.3.2 Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the record retention schedule, such as routine emails, or data not containing personal data that is generated on an informal basis as part of the day-to-day running of the organisation.

19.3.3 Both formal or official records and disposable information may contain personal data.

19.4 **Retention periods**

19.4.1 Any data listed in the record retention schedule must be retained for the amount of time indicated, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation – see below) calls for its continued retention. In the case of personal data, you should comply with the relevant principles set out at section 5 above. If you are unsure whether to retain a certain record, contact the Chief Officer or Operations Manager.

19.4.2 The record retention schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

19.4.3 Information about retention periods should be provided to Data Subjects as necessary or relevant in privacy notices.

19.5 **Storage, back-up and disposal of data**

19.5.1 Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up regularly and maintained off site.

19.5.2 The Operations Manager is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible.

19.5.3 The destruction of data must stop immediately upon notification that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation and the data could be relevant. Destruction may begin again once this requirement for preservation is lifted.

19.6 **Special circumstances**

19.6.1 We require all employees to comply fully with our record retention schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or are informed, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until you are informed that these records are no longer needed. Preserving documents includes suspending any requirements in the record retention schedule and preserving the integrity of the electronic files or other format in which the records are kept.

19.6.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Chief Officer or Operations Manager.

19.6.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

20. REPORTING A BREACH

20.1 The GDPR requires Controllers to notify any personal data breach to the applicable regulator and, in certain instances, the Data Subject, within 72 hours of having become aware of the breach.

20.2 We have put in place procedures to deal with any suspected personal data breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

20.3 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. You should immediately contact the person or team designated as the key point of contact for personal data breaches. Timely reporting is essential because of the stringent requirements under the GDPR for reporting breaches. You should preserve all evidence relating to the potential personal data breach.

21. GUIDANCE

21.1 This policy, procedure and guidance document should be read in conjunction with the related policies.

21.2 Any queries relating to the contents of this policy, procedure and guidance document should be referred to the Chief Officer or Operations Manager.

21.3 We are required to ensure registration with the Information Commissioner and an annual return is filed on behalf of the organisation by the Chief Officer. Further guidance is also available on the ICO's website: https://ico.org.uk/for-organisations/

22. DEFINITIONS

Word	**Definition**
automated decision-making	when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.
automated processing	any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance

	at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.
consent	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal data relating to them.
Controller	the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all personal data relating to our staff and personal data used in our business for our own commercial purposes.
criminal convictions data	means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.
Data Subject	a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.
data privacy impact assessment (DPIA)	tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programmes involving the processing of personal data.
EEA	the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
explicit consent:	consent which requires a very clear and specific statement (that is, not just action).
General Data Protection Regulation (GDPR)	the General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.
personal data	any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

personal data breach	any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.
privacy by design	implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
privacy guidelines	the Company privacy and GDPR related guidelines provided to assist in interpreting and implementing this policy and related policies, set out in Appendix 1.
privacy notices (also referred to as fair processing notices) or privacy policies	separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.
processing or process	any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties
pseudonymisation or pseudonymised	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
record retention schedule	the table setting out retention periods for formal or official records, set out at Appendix 2.
related policies	the Company's policies, operating procedures or processes related to this policy and designed to protect personal data, including the Computer and Telephone Systems: Acceptable Usage policy, Confidentiality policy, Information Sharing policy, Information Security Incident Reporting policy, Safeguarding policy and Whistleblowing policy
special categories of personal data	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

APPENDIX 1

GUIDANCE ON PROCESSING CERTAIN CATEGORIES OF DATA

1. PROCESSING CLIENTS' DATA

1.1 In addition to your responsibilities under the Act and the GDPR, your duty of confidentiality is fundamental to the relationship between Haven and its clients (being its beneficiaries). It exists as part of the contractual obligations to which we are subject, as a matter of professional conduct and is a condition of your employment.

1.2 Any disclosure of a client's confidences otherwise than in the proper performance of your duties or authorised by either the client or by law could render the business liable to a civil action by the client and/or by contracting parties.

1.3 We should treat our clients' information as confidential. However, this does not include information that we are instructed by them to disclose, or which we are compelled to disclose by law, for example, where fraud or other crime is involved. We may produce a client's file in certain circumstances, unless the client notifies us to the contrary and as an exception to the duty of confidentiality, in order to:

1.3.1 demonstrate our maintenance of professional standards; and/or

1.3.2 satisfy our auditors.

1.4 There are certain situations where of the need for confidentiality may be overridden, for example, where a court order has been made requiring disclosure or we have reason to suspect the client is involved in the commission of an offence. You must consult the Chief Officer or Operations Manager before making a disclosure on these grounds.

1.5 You also have a duty of confidentiality in relation to our own business and you must not disclose any information relating to our business and its activities to a third party without a manager's consent.

1.6 **Processing Employees' Data**

1.6.1 In the course of your recruitment and employment the business will collect, retain and process information consisting of personal data including sensitive personal data about you.

1.6.2 The purposes for which we hold any information about you are solely for administration and personnel management including (but not limited to):

(a) recruitment;

(b) appraisals;

(c) performance monitoring;

(d) promotion;

(e) training;

(f) career development;

(g) pay and remuneration;

(h) pension, insurance and other benefits;

(i) payroll;

(j) tax, national insurance and other deductions from pay;

(k) health and safety;

(l) discipline and grievances; and

(m) the review of our policies and procedures.

1.6.3 The business will also hold certain data about you defined by the GDPR as "special category data" comprising information as to:

(a) racial or ethnic origin; and

(b) physical or mental health or condition,

as well as the DBS reference number of an employee or candidate, which will be retained on file.

1.6.4 The business will process special category data and criminal conviction data about you solely for administration and personnel management purposes including (but not limited to):

(a) equal opportunities monitoring;

(b) suitability and fitness for work;

(c) sick pay and sick leave;

(d) absence control;

(e) maternity leave and pay;

(f) parental leave;

(g) paternity and adoption leave and pay;

(h) safe environment; and

(i) obligations under the Equality Act.

1.6.5 In addition to the above purposes, we may collect, hold and process data including special category data if it is necessary to do so for compliance with any statutory duty with which we are required to comply.

1.6.6 The information we hold for the above purposes will be retained for the duration of your employment by us. The purposes for which we hold any information about you after the end of employment are for use solely for any residual employment related matters including (but not limited to) the provision of job references, processing applications for re-employment, employment tax, matters relating to retirement benefits and allowing us to fulfill contractual or statutory obligations.

1.6.7 If necessary for the above purposes, we may transfer personal data to our insurers, bankers, medical and other professional advisers, Standard Life as the administrator/provider of our workplace pension scheme (or such other pension provider as we may from time to time engage) or your own pension provider and other organisations to which we have contracted.

1.6.8 We may monitor electronic communications by employees, including to websites, to ensure that these systems are being used in accordance with our computer policies and use of the telephone system to ensure that it is not subject to abuse.

1.6.9 The business will remind employees on an annual basis of the policy and procedural requirements and shall review understanding through the Internal Audit process.

1.7 **Handling and Storing Personal Data and Data Security**

1.7.1 As identified above, the business is obliged to ensure that personal data are secure. The appropriate level of security must be established having regard to the type of personal data being processed, the likelihood of disclosure and the harm that may result from any breach of security. Therefore, particular care should be taken of records which have a heightened sensitivity such as clients' files and employment records.

1.7.2 To safeguard against any unauthorised access to personal data in your possession, you should take steps to ensure that this personal data is kept

secure. Whilst we acknowledge that it is not always possible to keep personal data for which you are responsible securely within a filing cupboard, you must give consideration at all times to securing personal data against unauthorised access. It is important to recognise that information will not always be secure simply by virtue of being within the confines of Haven's premises and special care must be practised when taking files containing personal data outside the office environment, especially where the data is sensitive.

1.7.3 You must make sure that you do not disclose Personal Data to the wrong person. Please ensure that you verify that the individual who is asking for data is the Data Subject. You may not provide personal data about an individual to their spouse or family member without their specific permission.

1.7.4 One way you are required by us to ensure that personal data is stored securely and to safeguard against unauthorised access to personal data is to refrain from sending personal data relating to clients/residents, potential clients/residents, or former clients/residents by email under any circumstances.

1.7.5 Particular care should also be taken to ensure that Personal Data is properly and securely disposed of. Shredding bins have been made available throughout the business's offices in which you should place any confidential and/or personal data for disposal.

APPENDIX 2

DATA RETENTION SCHEDULE

1. Set out below are our standard time periods for retention of data. If data is not covered in the retention table below it is likely that it should be treated as day to day disposable data. However, if you come across any situation not covered in this schedule which you think should be, or you are unsure about the classification of data in this schedule, you should contact our Chief Officer or Operations Manager.

2. The retention periods below may be extended in the event that legal or regulatory proceedings are brought or an official investigation is launched. In these circumstances we will retain the data we consider relevant for as long as is necessary for the purposes of such proceedings.

Data Type (in general)	**Maximum Retention period**	**Reason/Comments**
Employee records		
Staff bank details	Record deleted immediately following cessation of employment (or immediately following final salary or other payment due, if later).	Necessary for us to fulfil our contractual obligations.
Proof of identification and proof of right to work (including visas)	Record kept for no longer than 36 months following cessation of employment, unless there is a statutory or other legal requirement to keep any such record for longer.	Necessary for us to fulfil our obligations as employer.
Equal opportunities monitoring data	Records kept for three years following cessation of employment.	Necessary for us to fulfil our obligations as employer.
Other Staff data	Records kept for duration of employment or engagement with us and for a period of seven years from the date your employment or engagement with us ends (and will be reviewed during that time to ensure its continued accuracy).	Necessary for us to fulfil our obligations as employer.
Other former staff data	Records kept for seven years following cessation of employment	Necessary for provision of references, forwarding of

Data Type (in general)	Maximum Retention period	Reason/Comments
	or engagement with us and will be reviewed during that time to ensure its continued accuracy.	information and other requirements ancillary to their past employment. Key records required as breach of contract claims may be brought for up to six years after cessation of employment or engagement. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Job applicant records		
Job applicants (unsuccessful)	Records of unsuccessful applicants kept for seven months after we have communicated to the relevant applicant the decision not to take their application forward unless otherwise agreed with the applicant to retain for a longer period.	Necessary to respond to and defend any claim made by job applicants and to demonstrate that the recruitment exercise has been conducted in a fair and transparent way and in accordance with our procedures. Where an extension to the seven month retention period is agreed, this will be in circumstances where we believe a future opportunity may arise for which we may wish to consider the applicant. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Job applicants (successful)	Personal data obtained during the recruitment process will be transferred to the individual's personnel file and held for the period(s) set out above.	Retained during employment and the post-employment period noted above

Data Type (in general)	Maximum Retention period	Reason/Comments
Client records		
Resident contact details	Records kept for duration of residence and for 12 months following cessation of residence (and will be reviewed during that time to ensure its continued accuracy), or for such longer period as required by local authorities or other agencies.	Necessary to comply with legal obligations
Resident support and behavior records	Records kept for duration of residence and for 12 months following cessation of residence, or for such longer period as required by local authorities or other agencies.	Necessary for us to administer our services. This period is necessary to comply with our legal obligations (such as submitting data and returns to contracting authorities). After such period, information about former residents is held by the relevant local authority and is available for us to access if required, for example to indicate compliance with contractual requirements, whose limitation period is six years.
Other clients' data	Records kept for the duration of their residence in our facilities and then in accordance with retention period for 'other former clients' data' set out below.	Necessary for us to administer our services.
Other former clients' data	Records kept for 12 months following cessation of residence.	Necessary for provision of references, to enable forwarding of information and other requirements ancillary to their past residence. After such period, information about former residents is held by the relevant local authority and is available for us to access if required, for example to

Data Type (in general)	Maximum Retention period	Reason/Comments
		deal with any claim brought against us within the limitation period.
Trustee records and governance records		
Trustees	Records kept for the duration of their trusteeship and for the period of seven years thereafter.	Necessary for the administration of the charity, including regulatory reporting requirements (see row below). This period is also necessary given the six year limitation period for breach of trust. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Former trustees	Records kept for seven years following cessation of trusteeship.	Necessary for regulatory reporting requirements, such as Charity Commission annual return, which can be submitted up to 9 months following the end of the financial year. This period is also necessary given the six year limitation period for breach of trust. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Third party records		
Staff next of kin details	Records kept for the duration of employee's employment or engagement or, for so long as that individual remains the employee's next of kin contact, whichever is	Necessary to help ensure the safety and wellbeing of an employee in an emergency.

Data Type (in general)	Maximum Retention period	Reason/Comments
	the earliest.	
Client next of kin details	Records kept for the duration of client's residence or, for so long as that individual remains the client's next of kin contact, whichever is the earliest.	Necessary to help ensure the safety and wellbeing of a client in an emergency.
Complaints records	Records kept for seven years following the last action in relation to the complaint	Necessary in the event of any claim or litigation brought. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Supplier records		
Supplier contracts	Records kept for seven years following cessation of contract where those contracts are executed as simple contracts, or 13 years where those contracts are executed as deeds.	Necessary as breach of contract claims may be brought for up to six years after cessation of services where the contract is executed as a simple contract, or 12 years where the contract is executed as a deed. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Supplier contact details	Records kept for seven years following cessation of contract where those contracts are executed as simple contracts, or 13 years where those contracts are executed as deeds.	Necessary as breach of contract claims may be brought for up to six years after cessation of services where the contract is executed as a simple contract, or 12 years where the contract is executed as a deed. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.

Data Type (in general)	Maximum Retention period	Reason/Comments
Financial and insurance records		
Accounting records	Records kept for three years from the date made.	Necessary to ensure compliance with the Companies Act 2006.
Insurance certificates	Records kept for 21 years.	Necessary to ensure records held if claim required to be brought in relation to that period of insurance.
Records of grant makers		
Potential grant-funders	Records kept until an application is made and is successful or unsuccessful, or for three years if no such application is made.	Necessary to enable us to retain a record of grant funding options to ensure a coherent grant funding strategy.
Grant funders in relation to which grant requests have been unsuccessful	Records kept for three years following rejection of grant application.	Necessary to inform further grant applications and to ensure a coherent fundraising strategy.
Grant funders in relation to which grant requests have been successful	Contractual documentation kept for seven years following the end of the grant term where executed as a simple contract, or 13 years where executed as a deed. Related records kept for the same period.	Necessary to enable compliance with the grant terms, support in other grant applications and (in the case of contractual documentation) necessary as claims may be brought for up to six years or 12 years following the end of the grant term where executed as a simple contract or deed (respectively).
Records of marketing and fundraising recipients		
Fundraising appeal recipients contact details	Records kept for so long as consent is valid.	The individual has provided consent for their data to be retained for marketing purposes.
Records of partner councils and service contractors		
Communications between us and the partner	Records kept for seven years following cessation of the contract	Necessary as breach of contract claims may be brought for up to

Data Type (in general)	Maximum Retention period	Reason/Comments
council/service contractor pursuant to the contract.	where the contract is executed as a simple contract, or 13 years where executed as a deed.	six years after cessation of services where the contract is executed as a simple contract, or 12 years where the contract is executed as a deed. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Other communications between Haven and the partner council/service contractor	Records kept for 7 years following last contact where the relevant contract between the parties is executed as a simple contract, or 13 years where the relevant contract is executed as a deed.	Necessary as breach of contract claims may be brought for up to six years after cessation of services where the contract is executed as a simple contract, or 12 years where the contract is executed as a deed. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation period is extended.
Data/information collected by us on behalf of the partner council/service contractor or obtained in pursuance of a contract with the partner council/service contractor	Records kept for so long as mandated by the partner council/service contractor.	Necessary in furtherance of the contract in place and/or the relationship with that party.
Contract with the partner council/service contractor	Records kept for seven years following cessation of contract where the contract is executed as a simple contract or 13 years where the contract is executed as a deed.	Necessary as breach of contract claims may be brought for up to six years after cessation of services where the contract is executed as a simple contract, or 12 years where the contract is executed as a deed. A grace period is required in the event that a claim is brought at the end of the limitation period or the limitation

Data Type (in general)	Maximum Retention period	Reason/Comments
		period is extended.