Data Protection Policy

Prepared By

Document Owner(s)	Project/Organization Role
Racheal Hoult	Information Compliance Officer (Executive Support and Communications Coordinator)
Stephanie Rushton	Business Services Director

Employment Manual Version Control

Version	Date	Author	Change Description
1.0	25/10/2023	Racheal Hoult	New version Data Protection Policy as per Data Protection People review recommendations.
1.2	09/09/2025	Racheal Hoult	Updated to reflect implementation of the Data Use and Access Act 2025 (DUAA)

1 Introduction and Scope

1.1 Scope

This Data Protection Policy sets out the organisation's commitment and approach to data protection and provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance. The policy's objectives are:

- To provides a clear frame of reference for employees to determine the organisation's standards, aims, and ideals in respect of data protection compliance.
- To provide information to data subjects, data processors, and the regulatory authorities about how the organisation approaches data protection compliance.

Unless otherwise stated this document applies to all **personal data** processed by PFH. It applies to any natural or legal person who process personal data for or on behalf of PFH including employees, volunteers, casual and temporary employees, directors and officers, external organisations employed as processors and any external organisations or individuals with whom PFH shares or discloses personal data. It also applies where PFH is a joint controller or where relevant, acts as a processor for another controller.

1.2 Background

The processing of personal data in the United Kingdom is regulated by law, principally the United Kingdom General Data Protection Regulation ("UK GDPR"), the Data Use and Access Act 2025 ("DUAA") and the Data Protection Act 2018 ("the Act"). Other laws inter-relate with the Act and the UK GDPR including but not limited to the Privacy and Electronic Communications Regulations (2003) ("PECR"). In addition, various guidelines, codes of practice, and case law contribute to the Data Protection Legislation. It is also possible that organisations are subject to the EU GDPR and other European legislation.

The Data Protection Legislation sets out legal responsibilities on all organisations processing personal data and provides for legal rights for the people whose data are being processed. It also sets out the offences, penalties and remedies. Penalties can be imposed on organisations processing personal data including fines of up to £17,500,000 or 4% of prior year global annual turnover whichever is the greater. There are a number of criminal offences set out in the Data Protection Legislation and individuals can be held accountable and be sentenced by the courts for offences under the Data Protection Legislation.

This Policy is a public statement describing this organisation's approach to complying with its legal responsibilities in the Data Protection Legislation and how it enables individual rights to be upheld and exercised.

2 Policy Statement

PFH is committed to compliance with all relevant Data Protection Legislation. The organisation will maintain a suite of policy documents setting out how it intends to implement management controls sufficient to ensure legal compliance with Data Protection Legislation and will ensure that these documents are reviewed periodically to a) test their adequacy in meeting the legal standards as they

change over time, and b) to test the organisation's compliance with them. The organisation will ensure that all relevant personnel and/or other persons it commissions to process personal data on its behalf, either directly or indirectly, have received appropriate and sufficient training in the application of the organisation's policies.

The management will ensure that sufficient and appropriate resources are available to ensure that the organisation meets both its legal obligations in respect of Data Protection Legislation and the standards that it sets through its policies.

The management will ensure that the organisation works within the 7 data protection principles and that it will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

The organisation will uphold the rights and freedoms of people conferred on them by the Data Protection Legislation. It will ensure that those rights and freedoms are appropriately taken into account in the decisions it takes which may affect people and will ensure that it has sufficient controls in place to assist people who wish to exercise their rights.

This policy applies to all of the organisation's activities or operations which involve the processing of personal data.

This policy applies to anyone who is engaged to process personal data for or on behalf of the organisation including: employees, volunteers, casual and temporary staff, directors and officers, and third-parties such as sub-contractors and suppliers, and anyone who the organisation shares or discloses personal data with/to.

3 Responsibilities

3.1 Data Controller

PFH is the legal data controller under the Data Protection Legislation.

3.2 Chief Executive

The Chief Executive is the accountable officer responsible for the management of the organisation and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and thus maintaining confidentiality is pivotal to the organisation being able to operate.

3.3 Directors

Each Director in their respective areas of responsibility, must ensure that all staff members are aware of this policy, other relevant policies and procedures, and their responsibilities concerning the processing of personal data. Each Director must ensure this policy is adhered to.

3.4 Information Compliance Officer

The organisation shall nominate an Information Compliance Officer who shall be responsible for maintaining the policies, guidance and training needed to ensure the organisation is compliant with

Data Protection Legislation. The Information Compliance Officer shall monitor and report to the Senior Leadership Team in respect of compliance with the policies and procedures, arrange for the investigation of any security incidents, and maintain suitable records of processing activities. They may co-opt other individuals to assist with the management of data protection obligations. The Information Compliance Officer shall manage the appointed contract with the external data protection consultants (currently Data Protection People), ensure 3 yearly reviews of this policy and associated policies and procedures, monitor the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporate relevant changes into the Organisation's policy in a change-controlled manner.

3.5 Operational Managers

Operational Managers are responsible for ensuring that all data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy and how it applies to their job role and sufficiently trained to carry out their duties in compliance with this policy.

Operational Managers are also responsible for understanding what personal data is used in their business area and how it is used, who has access to it and why. As a result, they are able to understand and address risks to the data and the organisation.

Operational Managers may delegate day-to-day responsibility for compliance within their team, subject to other HR policies and ensuring that all staff are appropriately trained.

3.6 Data Champions

Information assets are identified in the PFH Information Asset Register which is maintained by the Information Compliance Officer and Data Champions (usually the Operational Manager for the business area). The Data Champion has primary operational responsibility for compliance with data protection legislation and good practice in respect of assigned information assets.

The Data Champion role is to understand what personal data is used in their business area and how it is used, who has access to it and why. As a result, they can understand and address risks to the data and the organisation within the Information Governance Framework.

Data Champions may delegate day-to-day responsibility for compliance within their management hierarchies, subject to other HR policies and ensuring that all staff are appropriately trained.

3.7 HR Manager

The HR Manager holds operational responsibility for compliance with data protection compliance in relation to the management of its work force including recruitment and retention. In liaison with the Information Compliance Officer the HR Manager is responsible through the staff performance management framework for ensuring that adequate training is provided to all employees to ensure data protection compliance.

The HR Manager has operational responsibility for compliance with data protection policies and best practice in relation to HR policies and procedures including recruitment and retention.

3.8 IT Management

The IT Manager holds operational responsibility for compliance with data protection legislation and best practice for information security. Further guidance is available in the association's IT policies and procedures. Employees, volunteers, casual/temporary workers, directors and officers etc.

Anyone who is directly engaged by the organisation to undertake data processing activities including but not limited to employees, volunteers, casual/temporary workers, directors and officers etc. involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they are undertaking or witnessing should contact the Information Compliance Officer. Individuals are expected to complete appropriate training from time to time. Everyone within the Organisation has a duty to respect data subjects' rights to confidentiality.

Disciplinary action and / or penalties could be imposed on staff for non-compliance with relevant policies and legislation.

3.9 Partner & Third-Party Responsibilities

Any Third Party or organisation that is commissioned to process data or receives data from PFHor is able to access any personal data which is within the custody of PFH **must** complete a Service Provider Data Processing Agreement. This must be recorded on the Service Provider Data Processing Agreement Tracker (all available within Data Protection - Published General Association Folder).

4 Data Protection Policy Detail

4.1 Data Protection Officer (DPO)

The organisation has determined that it is not required to designate a Data Protection Officer and has documented the rationale underpinning its decision which it shall keep under periodic review.

4.2 Fair Lawful and Transparent processing

The processing of all personal data by the organisation will only be undertaken in a fair, lawful and transparent manner meaning:

Fairness – no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person from whom data are being collected and to the people who the data are about if personal data are collected from sources other than the data subject. All privacy information and any changes to privacy information must be approved by the **Information Compliance Officer**.

Lawfulness – no data collection activities will be undertaken or commissioned without there being a lawful basis for the data processing activities intended to be applied to the personal data. The **Information Compliance Officer** is responsible for determining the lawful grounds for processing. Where the lawful grounds are consent, the consent policy will apply. Where the lawful grounds are legitimate interests a legitimate interests assessment (LIA) will be undertaken and documented. Under changes within the DUAA there are now processing activities that are considered to be a "Recognised legitimate interest" where this is the case we will not document an LIA but will ensure that it is documented that we rely on a recognised legitimate interest within our RoPA. Where the

lawful grounds are a task carried out in the public interest or in the exercise of official authority vested in the organisation, a public interests assessment (PIA) will be undertaken and documented. Where the lawful grounds are a legal obligation, the relevant legislation shall be cited and appropriately documented.

Each **Data Champion** is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control, that the consent policy is adhered to, and a LIA/PIA is properly undertaken where necessary. The **Information Compliance Officer** will provide or seek advice regarding lawful processing conditions and a register of the lawful grounds for all of the organisation's processing activities involving the processing of personal data is included within the Information Asset Register.

Transparency – the organisation will endeavour to provide sufficient information about how personal data is being processed to enable sufficient transparency about its handling of personal data. The **Information Compliance Officer** shall periodically review the apparent transparency.

4.3 Data processing purposes

Personal data shall only be collected, created or otherwise obtained for specific, explicit and legitimate purposes. No data processing shall be undertaken or commissioned without the completion of a service provider processing agreement, consultation with the Information Compliance **Officer** and/or relevant Manager who shall review, and were necessary, update the Information Asset register with the data processing activities and their purpose. **Data Champions** are responsible for ensuring that all of the data processing activities that they undertake and/or commission are recorded. No personal data shall be used for any purpose other than that which it was collected and/or created for without consultation with the **Information Compliance Officer**.

4.4 Data minimisation

The organisation will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collects. **Data Champions** are responsible for ensuring that no un-necessary, irrelevant or unjustifiable personal data are collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The **Information Compliance Officer** will provide advice regarding the justification of personal data collected or created.

4.5 Data accuracy

The organisation recognises that the accuracy of data is important, and that some data is more important to keep up to date than others. The organisation will use its reasonable endeavours to maintain data as accurate and up to date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date.

All employees are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in are maintained accurate and up-to-date and that personal data whose accuracy cannot reasonably be assumed to be accurate and up to date are treated appropriately through erasure or anonymisation. The **Information Compliance Officer** will provide advice regarding data accuracy.

4.6 Data retention

The organisation will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymization.

All employees are responsible for determining the retention period for ensuring adherence to the organisations retention policies for personal data under their control or sphere of influence.

Data retention is a vitally important issue as both the over-retention and under-retention of personal data could have a detrimental impact on both the data subject and the organisation.

4.7 Information security

The organisation will ensure that any personal data that it processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In particular, an information security management policy (ISMP) will be maintained setting out specific policies in relation to maintaining personal rights, confidentiality, availability and integrity. The **IT Manager** will be responsible for the formulation of the ISMP.

4.8 Children's data

Special measures will be taken by the organisation if it processes personal data relating to children under the age of 13 including the nature of privacy information provided and approach to information rights requests.

4.9 Personal data relating to criminal convictions and offences

If the organisation is processing personal data relating to criminal convictions and offences, it shall implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

4.10 Special categories of personal data

Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The organisation shall not process special categories of personal data unless it is necessary. Where the processing of special categories of personal data is necessary, Data Champions shall ensure that the lawful grounds for such processing are documented within the Information Asset Register and shall maintain a periodic review of the necessity to processing the special categories of personal data.

4.11 Consent

The organisation will interpret consent to be as defined in the GDPR and that any consent shall not be valid unless:

- there is a genuine choice of whether or not to consent.
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;
- the organisation can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully;
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent;

The organisation recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. The organisation recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

4.12 Record keeping and accountability

To fulfil its responsibility to be able to demonstrate compliance with Data Protection Legislation as well as in support of the policy on transparency the organisation will maintain records of the processing activities that it controls, undertakes or otherwise commissions (Information Asset register) as required by the Data Protection Legislation and specifically those required in Article 30 of the GDPR.

The **Information Compliance Officer** shall be responsible for maintaining the Information Asset Register and provision to the Information Commissioner's Office on demand as required.

The organisation shall strive to maintain additional documentation capable of demonstrating accountability as necessary: the organisation's retention schedule determines what records should be kept, for how long and in what format and will be reviewed at least every 3 years.

4.13 Information rights policy

The organisation recognises the legal rights of those whose data it is processing or intends to process and will ensure that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to ensure that the organisation is able to recognise information rights requests and handle them appropriately when they are exercised. These rights include:

- Right to information about data processing operations
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing

- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data
- The right to complain to the ICO and the right to a judicial remedy and compensation
- The organisation shall maintain procedures setting out how information rights requests are to be handled and ensure that all relevant people are made aware of it.

4.14 Personal Data Breaches policy

The organisation will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this personal data breaches policy.

All employees and individuals with access to personal data for which the organisation is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach. The organisation will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The Data Breach Reporting Procedure sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach.

The **Information Compliance Officer** shall be responsible for maintaining the Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

4.15 Data Processors

The organisation reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors may be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation.

Employees wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The Information Compliance **Officer** shall provide advice and guidance in respect of this.

A Service Provider Processing Agreement shall be completed by the data processor and Recorded on the Service Provider Data Processing Agreement Tracker, with the document saved in the agreements folder located in Data Protection Folder within the Published General Association Drive.

No employee is permitted to commission or appoint a third party to process data on behalf of the organisation without adhering to this policy. **The organisation as a data processor**

Where the organisation acts as a data processor it shall ensure it retains records of processing activities which record at least the information required under Article 30(2) of the GDPR for each

controller it acts on behalf of. The organisation shall ensure that it has an appropriate agreement in place with each data controller and shall ensure that its employees, volunteers, staff and contractors, receive appropriate training to enable them to ensure compliance with the instructions and contractual terms of each data controller.

4.16 Data sharing, disclosure and transfer

The organisation will only share personal data with or otherwise disclose personal data to other organisations and third parties where there is a legal basis for doing so and the data sharing is necessary for specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation being in place. Data sharing agreements must be saved in the relevant folder located in Data Protection Folder within the Published General Association Drive and recorded on the Service Provider Data Processing Agreement Tracker. Appropriate risk assessments will be undertaken prior to any data sharing taking place on those with whom we intend to share personal data. This policy extends to appointing others to process personal data on our behalf, sharing personal data with organisations, and providing information to ad-hoc requests for information such as those which may be received from the police and other authorities.

The organisation will provide Information to all employees setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Disciplinary action will be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer.

4.17 Internationalisation of personal data

The organisation will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that the organisation undertakes or commissions whether directly or indirectly must be approved by a member of the Senior Leadership Team and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK Government;
- The territory into which the data are being transferred is within the European Economic Area;
- The territory into which the data are being transferred has a decision with regard the adequacy of its data protection regime (Adequacy Regulations) issued by the UK Government;
- The transfer is made under the unaltered terms of an International Data Transfer Agreement (“IDTA”) issued by the Information Commissioner for such purposes and where required a Transfer Risk Assessment (“TRA”) issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the UK Government;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

Where necessary a risk assessment will be undertaken on any third country the organisation intends to transfer personal data to and supplementary measures will be implemented as necessary to ensure adequate protection of personal data.

4.18 Risk assessment

The organisation will adopt a risk-based approach to processing personal data ensuring that it assesses any risks to privacy or to the rights and freedoms of people before commencing or commissioning or changing data processing activities. Where necessary it shall, as a minimum, ensure that a data protection impact assessment (DPIA) is undertaken where required by Data Protection Legislation and/or when one is deemed to be desirable by the Senior Leadership Team.

The organisation will maintain a procedure setting out how data protection impact assessments are to be carried out and documented and ensure that appropriate resources are available to advise on DPIAs.

The **Information Compliance Officer** is responsible for maintaining a register of data protection impact assessments that have been undertaken by the organisation and for its periodic review.

4.19 Training and awareness

The Organisation will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. **The Information Compliance Officer and HR Manager** shall determine the training needs of Board Members and Staff and ensure that appropriate data protection awareness training is regularly provided.,

4.20 Continuous Improvement

The organisation will undertake 3 yearly reviews of this and associated policies and procedures. All identified data breaches will be reported to the Audit and Risk Committee.

4.21 Data protection by design and by default

The organisation shall strive to foster a culture of data protection by design and by default in all of its data processing activities. It shall ensure that measures are in place to encourage all those involved in data processing activities to adopt a model of continuous improvement to the technical and organisational measures that implement the data protection principles and safeguards into processing activities. The organisation shall strive to ensure that by default, only personal data which are necessary for each specific purpose of the processing are processed and that the extent of the processing, period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

5 Glossary

Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Data Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Data Subject	any living individual who is the subject of personal data held by an organisation;
Data Champions	The person responsible for the instigation or on-going maintenance of a data process or data processing operation;
Personal Data	means any information relating to an identified or identifiable living individual;
Identifiable living individual	means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;
Personal identifiable information (PII)	means personal data.
Special Categories of Personal Data	means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Information Incident	means an identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously

	unknown situation which may be relevant to the security of information;
Information Security Event	an occurrence in a service, system, or network that indicates a possible breach of information security. This includes breaks in policy, failure of controls, or other previously unknown situations;
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Risk	The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood;
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects;
Corporate Data	Corporate data relates to any sensitive corporate information including meeting schedules, agendas and minutes of meetings; financial accounts; contracts; and organisational policies and procedures;
Recipient	means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
Third-party	means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
Third Country	means a territory that is not the United Kingdom in the UK GDPR and means a territory that is not a Member State of the European Union in the EU GDPR;
Profiling	is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of

	profiling, of measures based on profiling and the envisaged effects of profiling on the individual;
Consent	means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data;
IAR	means information asset register: a register of information assets;
Information Asset	data or other knowledge that has value to an organization.

6 Document Control and approval

This Policy will be disseminated to all staff

including all new starters as part of their induction process. Managers will be responsible for keeping staff up-to-date with any changes to this Policy.

6.1 Approval

Name Position

Signature: