

Information Governance Policy

IG01 Information Governance Policies

May 2024

**Contents**

[1 Introduction 2](#_Toc167095787)

[2 Scope and Purpose 2](#_Toc167095788)

[3 Definitions 2](#_Toc167095789)

[4 Information Governance 3](#_Toc167095790)

[5 Document and Records Management 4](#_Toc167095791)

[5.1 The Importance of Documents and Records 4](#_Toc167095792)

[5.2 Records and Information Life Cycle 5](#_Toc167095793)

[6 Data Confidentiality 7](#_Toc167095794)

[6.1 Confidentiality and clear desk principles 7](#_Toc167095795)

[6.2 Disclosing personal data 8](#_Toc167095796)

[6.3 Working outside an MHA location 8](#_Toc167095797)

[7 Information Security 9](#_Toc167095798)

[8 Archiving 11](#_Toc167095799)

[8.1 Introduction 11](#_Toc167095800)

[8.2 On-Site Archiving 11](#_Toc167095801)

[8.3 Off-Site Archiving 12](#_Toc167095802)

[8.4 Retrieval Of Records (off-site) 13](#_Toc167095803)

[8.5 Archive Destruction (on-site & off-site) 14](#_Toc167095804)

[9 Roles and Responsibilities 14](#_Toc167095805)

[10 Training and Monitoring 17](#_Toc167095806)

[11 Communication and Dissemination 17](#_Toc167095807)

[12 Resources 18](#_Toc167095808)

[13 Appendices 18](#_Toc167095809)

[13.1 Appendix 1: Document and Records Management Guidance 18](#_Toc167095810)

[14 Version Control 22](#_Toc167095811)

1. Introduction
   1. Colleagues will be aware of, understand and know how to implement Information Governance as relevant to their role to ensure that Personal Data is processed lawfully, confidentially, and securely.
2. Scope and Purpose
   1. All MHA colleagues and third-party organisations that process Personal Data for or on behalf of MHA, are required to:
   * Ensure that all colleagues are aware of their roles, responsibilities and accountability and fully comply with the Legislation as described in this and other Information Governance (IG) policies.
   * Create and maintain a level of awareness of the need for confidentiality and information security as an integral part of MHA’s day to day business.
   * Protect information assets under MHA’s control.
3. Definitions

| Term | Definition |
| --- | --- |
| **Colleagues** | An Identifiable Natural Person who works part-time or full-time for MHA under a contract of employment (colleagues), volunteer agreement (volunteer) or as an independent contractor. |
| **Data Protection Legislation,**  **Legislation** | This includes: the UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR) as updated from time to time. |
| **Data Subject** | An identifiable living person. For MHA this is past & present, living: colleagues, residents, family members and supporters or any person for whom MHA processed or has processed personal data |
| **Document**  (see Record) | A piece of writing that contains information, e.g. a recipe. |
| **IT Policy** | The IT policy (Computer Use Policy) and IT guidance, which will be updated from time to time. |
| **Legal Hold (or Litigation Hold)** | The need to ensure that documents, relevant to the subject matter of a pending or anticipated lawsuit, investigation, or inquiry, are kept safe from being edited, deleted, or destroyed. |
| **Personal Data** | Any information (including opinions and intentions) which relates to a Data Subject. |
| **Process, Processed, Processing** | Any operation or set of operations performed on Personal Data or on sets of Personal Data, by automated or manual means. Operations may include collect, record, organise, sort, store, edit, retrieve, use, disclose, combine, restrict, erasure, or destroy. |
| **Record**  (see Document) | A piece of writing that contains information that can be used as evidence, e.g. that a recipe was followed on a specific date, food temperatures were checked, food was served to x, y & z. |

1. Information Governance
   1. The framework (policies and guidance) governing the use of personal data in a secure manner and to appropriate legal, ethical, and quality standards. It provides a consistent way for colleagues to deal with many different information handling requirements including:
   * Using personal data of colleagues, living residents and family members
   * Using personal data of deceased residents
   * Using personal data for marketing purposes
   * Managing the risks of systems and processes that use personal data
   * Dealing with incidents involving personal data
   * Retention of records and archiving (including business data)
   * Demonstration compliance with the Legislation.
   1. The aim of the framework is to make the most of the information processed by MHA by ensuring that data is:
   * Obtained fairly and lawfully.
   * Held securely and confidentially.
   * Recorded accurately and reliably.
   * Used effectively and ethically.
   * Shared / disclosed appropriately and lawfully.
   1. To protect the information processed from all threats, whether internal or external, deliberate, or accidental, MHA will make sure:
   * Appropriate training will be available to all colleagues.
   * Information will be protected against unauthorised access.
   * Confidentiality of information will be assured.
   * Integrity of information will be maintained.
   * Information will be supported by the highest quality data.
   * Regulatory and legislative requirements will be met.
   * Business continuity plans will be implemented.
   1. All breaches of information security, actual or suspected, will be reported to, and investigated by the Data Protection Officer.
2. Document and Records Management

The Importance of Documents and Records

* + 1. All colleagues and people using our services would rightly expect that MHA maintains excellent records on its activities and decisions that affect them.
    2. A Record can be in various formats including email, paper, digital, social media, videos, and telephone messages.
    3. A Record may contain Personal Data, but may not contain Personal Data, e.g. building records.
    4. Records are created to provide information about what happened, what was decided, how to do things, etc.
    5. Records management is about controlling Records to ensure they are accurate, up to date, providing reliable evidence of actions and decisions and are accessible when needed.
    6. The law requires certain records are kept for a defined retention period, as detailed in MHA’s Retention Schedule. It sets out the classes of records which MHA retains and the length of time these are retained before a final disposal. It applies to information regardless of its format or the media in which it is created or might be held.
    7. Colleagues, as part of their daily work:
  + Must complete records as close as possible to the time of the event,
  + Must ensure that handwritten records are legible,
  + Must manage records taking into consideration the sensitivity of the data,
  + Must file records, sorted, and in the correct location,
  + Must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the Legislation, and
  + Must apply the correct retention periods to records.

Records and Information Life Cycle

* + 1. Records are used on a daily basis for internal purposes to help make decisions, provide evidence, etc. The diagram below shows the 5 steps in the Records Life Cycle:
  + **Stage 1 - Creation and Receipt:** This part of the life cycle is pen to paper, making an entry into a database or starting a new electronic document. It can be created by internal colleagues or received from an external source.
  + **Stage 2 – Distribution:** Distribution is managing the information once it is created or received whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied, ready for use.
  + **Stage 3 – Use:** This stage takes place after information is distributed. This is when records are used on a day-to-day basis to help generate organisational decisions, document further action, or support other MHA operations.
  + **Stage 4 – Archiving:** Archiving is when records are not used on a day-to-day basis and may be stored off-site. Even though they are not used on a day-to-day basis, they will be kept for legal or financial reasons until they have met their retention period. The archiving phase includes filing, transfers, and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records must not be removed from site (except for external archiving to an approved supplier); if required, the information should be copied and tracked to ensure no amendments are made.
  + **Stage 5 - Disposition / Disposal:** Disposition is when a record is less frequently accessed, has no more value to MHA or has met its assigned retention period (see Retention Schedule). It is then reviewed and if necessary, destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met, there may be a legal requirement to keep them for longer, e.g. due to an active investigation.

A diagram of a diagram

Description automatically generated

1. Data Confidentiality

Confidentiality and clear desk principles

* + 1. All colleagues must make sure that the following principles are adhered to:

1. Personal Data must be protected against improper disclosure.
2. Access to Personal Data must be on a need-to-know basis.
3. Conversations involving Personal Data must be help in private.
4. Exercise caution when having a confidential telephone call. Ask people to leave the room and/or close doors.
5. Computer access is kept secure. Passwords must not be shared. Computers must be locked when you are not in front of your computer.
   * 1. MHA is responsible for protecting all the Personal Data it Processes and must always be able to justify any decision to share information.
     2. Access to rooms and offices where computers are present or Personal Data is stored must be controlled, with need-to-know access. Doors must be locked, or measures must be in place to prevent access to, or viewing of, Personal Data by unauthorised parties.
     3. All colleagues must clear their desks at the end of each day. They must ensure all records containing Personal Data are locked away.
     4. Records must be filed and locked away when not in use.
     5. Unwanted printouts containing Personal Data must be disposed of securely.
     6. Contracts of employment include a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in disciplinary action up to and including dismissal. Colleagues may also be held personally liable.

Disclosing personal data

* + 1. Personal Data must only be disclosed where there is a lawful basis for doing so, as detailed in the Data Protection Policy.
    2. When Personal Data has been anonymised, i.e. all identifiable data has been removed, it is no longer Personal Data. Discuss with the DPO to ensure it is anonymised. It can therefore be disclosed unless there is another business reason for not disclosing it.
    3. If colleagues have any concerns about disclosing Personal Data, they must discuss this with their Line Manager and / or the Data Protection Officer.

Working outside an MHA location

* + 1. There will be times when colleagues may need to work from another location (e.g. at home) or whilst travelling (e.g. on the train). Extra diligence is required to ensure paper records are not read, computer screens are secure (e.g. no one can look over your shoulder) and confidentiality is maintained during telephone calls.

1. Removing paper documents that contain Personal Data from an MHA location is discouraged. If necessary, colleagues must:
2. keep it on their person at all times whilst travelling
3. ensure that it is kept in a secure place if taken home or to another location, e.g. in a locked draw or cabinet.
4. Take only the necessary personal Data for the work they intend to do while away.
   * 1. When working away from an MHA location, colleagues must ensure that their working practice complies with MHA’s policies and procedures.
     2. If Personal Data is being transported:
5. Your line manager must know what is being transported and the destination
6. sealed non-transparent containers must be used, e.g. windowless envelopes, suitable bag with a lock.
7. Personal Data is kept out of sight whilst being transported.
   * 1. If colleagues need to take Personal Data home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family / friends / visitors must not be able to see the content or have any access to the information.
     2. Colleagues must not forward any records containing Personal data to their personal, non-MHA, email account.
     3. Colleagues may only use a privately owned computer or device, as per the IT Policy.
8. Information Security
   1. The aim of Information Security is to preserve:
   * **Confidentiality:** Access to data must be confined to those with appropriate authority - i.e. need to know access.
   * **Integrity:** Information must be complete and accurate. All systems, assets and networks must operate correctly, according to specification.
   * **Availability:** Information must be available and delivered to the right person, at the time when it is needed.
   1. Access to areas containing Personal Data must be restricted to users who have an authorised business need to access the data.
   * **IT Access:** Access to computers and devices must be controlled by passwords (computers) or pins (phones & tablets) as per the IT Policy. IT systems, whether accessed via MHA’s network or the internet, must be protected according to the IT Policy, where possible Role Based Access Controls (RBAC) must be utilised.
   * **Building Access:** Access to building should be protected by pin or fob access, or by internal colleagues allowing access to recognised, authorised individuals.
   * **Cupboards, cabinets and draws.** Where these storage solutions are used to store Personal Data, they should be protected by a key or pin device, with access only being granted on a need-to-know basis.
   1. All colleagues that process Personal Data must ensure that the data they process is accurate and up to date to maintain the integrity of the data. If data exists in multiple areas (IT or paper) and the integrity falls under question, the colleague must report this to their line manager who must determine which data is correct and ensure that all systems are updated.
   2. If a colleague becomes aware that Personal Data is not accessible, they must inform their line manager and work to resolve the issue, e.g.:
   * If paper records cannot be located, where possible a new set should be created.
   * If access to an IT system is interrupted, the IT Helpdesk must be informed.
   * If data has been deleted in error, the IT Helpdesk or system owner should be contacted and asked to restore from backup.
9. Archiving

Introduction

* + 1. Archiving is a two or three stage process. Two stages if there is off-site is not required, three stages where off-site storage is required. The stages are:
  + **Stage 1**: Onsite archiving of records
  + **Stage 2**: Off-site archiving of records (including retrieval)
  + **Stage 3**: Disposal of archived records once retention period met
    1. All services and departments must have a documented procedure detailing the archiving procedure. This should include colleagues authorised to access the archives (typically: manager, deputy & administration manager/administrator), the process for managing the archives and where the archive logs are located. All authorised colleagues must have access to this document, or a copy of the latest version.

On-Site Archiving

* + 1. **Note:** All archived paper records must be logged electronically, so the complete records can be located with ease. The log must be saved in an easily identifiable folder so that the log can be located if the primary user is not available. The service or department manager must have access to the log.
    2. **Note:** As per HP005, while time a person is living in an MHA service, colleagues must be able to access that person’s records, i.e. they must not be sent to off-site storage.
    3. The physical archive location must be locked and only accessible by authorised colleagues, typically the service manager and deputy and the Administration Manager or the Administrator responsible for archiving.
    4. A risk assessment must be carried out considering the risks regarding the archive location, i.e. access, fire, water ingress, damp, and pests.
    5. Each box should only contain one type of record, e.g. a box should not contain colleagues and corporate finance records.
    6. The room or storage area used for archives should keep separate different types of records, i.e. keep care records together, colleagues records together, admin & finance records together, etc. Boxes must not be stored on the floor.
    7. Colleagues must:
  + Keep an electronic logbook of archive boxes. Archive log must be used. From June 2024 freeze previous logs, not adding boxes but keeping records up to date. Start a new log using the latest Archive log.
  + Not overfill the box making it too heavy or putting excess strain on the sides of the box which may cause it to become misshapen and the lid not to fit properly - only fill the box up to the handle hole.
  + Place a contents list inside the box so that contents can easily be located. The insert now forms part of the archive log file.
  + Place Archive Box Labels on the exterior of the box identifying the: box number, source of the records (care home, housing scheme or Epworth House department), date of archive, name of inserter and due date of destruction.

Off-Site Archiving

* + 1. **Note:** Before off-site storage is used it needs to be determined if it is required. The typical reason is due to lack of space. However, it also needs to be determined if the records need to be retained. Consult the Retention Schedule, an appropriate manager or the Data Protection Officer for guidance.
    2. **Note:** If there is an active investigation or potential investigation involving the records that have been sent to off-site storage, the records must be recalled.
    3. Boxes must be labelled and contain records with the same destruction year.
    4. Boxes will be collected by an external courier for delivery to MHA’s off-site storage solution.
    5. Records can be retrieved when required using the allocated reference information.
    6. The process for off-site archiving is an extension of the on-site archiving process detailed in section 2. The addition being that the log must detail that the box has been sent to off-site storage. The box will be collected by a courier, who will provide additional labels with barcodes and assume responsibility for the archive.
    7. Colleagues must add the information provided by the courier or storage company to the archive log.
    8. Any records required by safeguarding, police, the coroner or for any other legal reason (e.g. an insurance claim) are deemed to have a “Legal Hold” on them. They must be retained at the service or Epworth House.

Retrieval Of Records (off-site)

* + 1. If a request for records is made by anyone the manager must pass the request (e.g. letters or emails) to the Data Protection Officer who will log and process the request.
    2. All retrieval requests must be documented by the host location and be recorded in their log. Boxes can be sent direct to the Data Protection Officer at Epworth House as appropriate.
    3. **Procurement will:** manage the relationship with the external storage company, have access to the details of what boxes have been archived by each location and be able to provide guidance on depositing and retrieving records. Procurement will not hold details of the box contents; these must be held at the sending location.

Archive Destruction (on-site & off-site)

* + 1. **Note:** If there is an active investigation the records involved are deemed to have a “Legal Hold” on them. They must be retained at the service or Epworth House. The retention period will start from the date the case is closed.
    2. **Note:** The owner of the records is responsible for knowing when records need to be destroyed. When records in an off-site storage location have reached their destruction date, the company needs to be informed to destroy the records and provide proof of secure destruction. This could be scheduled twice a year, e.g. January & July.
    3. Destruction must be by a certified company with whom MHA has a contract (contact Procurement for assistance) or using a shredder rated at Security Level P-4. This will typically provide small crosscut shredding that cannot be reconstructed.

1. Roles and Responsibilities

| Role | Responsibilities |
| --- | --- |
| **All Colleagues** | All colleagues must understand and apply to the Information Governance policies. |
| **Senior Managers** | Shall be individually responsible for the security of their physical environments where information is processed or stored. They are responsible for:   1. Ensuring that their team are aware of the information security policies, procedures, and user obligations applicable to their area of work. 2. Determining the level of access to be granted to specific individuals. 3. Ensuring colleagues have appropriate training for the systems they are using. 4. Ensuring that any data breaches are reported to the Data Protection Officer. |
| **Information Asset Owners (IAO)** | An information asset is any piece or collection of information stored by MHA and processed as a single unit - e.g. colleagues’s personal file, resident’s care record. It is something we can’t replace without cost, time, skill, and resources.  All service managers (CH, RL & MHA Communities) are IAOs. All department heads are IAO. IAOs are responsible and accountable for the security and processing of all their information assets, they will:   1. Lead and foster a culture that values, protects, and uses the information assets lawfully. 2. Know who has access to the assets, and why, ensuring use is monitored and compliant with policy. 3. Understand and address risks to the asset and provide assurance to the SIRO. 4. Ensure there is a lawful basis for processing and for any disclosures.   Maintain adequate records the assets that are processed. |
| **Head of Talent Acquisition and Shared Services** | The Head of Talent Acquisition and Shared Services is responsible for ensuring that the contracts of all colleagues (permanent and temporary) are compliant with the requirements of information governance and that data protection is included in inductions. |
| **Associate Director of IT** | 1. Develop IT policies that implement best business practice, ensuring they are applied throughout the business. 2. Ensure effective management and security of MHA’s IT infrastructure and equipment. 3. Responsible for and being the point of contact for IT security within MHA. 4. Monitoring potential and actual security breaches, informing the DPO as appropriate. 5. Develop and implement an IT Disaster Recovery Plan. |
| **Caldicott Guardian** | The **Senior Nurse Advisor** is the Caldicott Guardian for MHA. The Caldicott Guardian will:   1. Work alongside the DPO to make sure that the personal information about people who use MHAs services is used legally, ethically, and appropriately and that confidentiality is maintained in relation to the storage, management and sharing of this information. 2. Provide leadership and informed guidance on complex matters involving confidentiality and information sharing regarding personal information for MHA’s residents. 3. Play a key role in ensuring that MHA satisfies the highest practical standards for handling the person information of people receiving care and support from MHA. 4. Apply the eight Caldicott Guardian Principles 5. Act as the conscience of MHA, providing impartial and independent advice. 6. Represent and champion information governance requirements and issues at senior management team and board level where appropriate, being and integral part of the overall information governance framework. 7. Play a key role in advising and ensuring that the Caldicott Principles are applied in digital and paperless systems. |
| **Data Protection Officer (DPO)** | MHA will ensure that there is always one person with overall responsibility for data protection, the DPO.  The DPO will:   1. Implement policies and procedures to embed the data protection principles and the rights of Data Subjects. 2. Ensure data protection training is provided to all colleagues and provide additional guidance and support as required or requested. 3. Keep records as required by the data protection legislation. 4. Risk assess each breach/incident and log with the ICO, as necessary. 5. Inform the Board of breaches or incidents that are reportable to the ICO. |
| **Senior Information Risk Owner (SIRO)** | The **General Counsel /** **Company Secretary** is responsible for information risk within MHA and advises the Board on the effectiveness of information risk management across the Organisation. The SIRO will -   1. Implement and lead MHA’s Information Governance Risk Assessment and Management processes. 2. Advise the Board on the effectiveness of information risk management across MHA.   Receive training as necessary to ensure s/he remains effective in the role as SIRO. |
| **Chief Executive Officer (CEO)** | Overall responsibility for strategic and operational management, including ensuring that MHA’s policies comply with all legal, statutory, and good practice guidance requirements. |

1. Training and Monitoring
   1. All colleagues must complete the following within three months of commencement of employment and annually thereafter, achieving a “pass” grade:
   * Confidentiality and Information Handling, and
   * Cyber Security Awareness
2. Communication and Dissemination
   1. This policy is disseminated and implemented within all MHA services through MHA’s channels of communication.
   2. Each colleague’s line manager must ensure that all teams are aware of their roles, responsibilities.
   3. This policy will be available to the people we support and their representatives in alternate formats, as required.
   4. Queries and issues relating to this policy should be referred to the Standards and Policy Team [policies@mha.org.uk](mailto:policies@mha.org.uk).
3. Resources
   1. **MHA policy documents, procedures, and guidance:**
   * Retention Schedule [IG01a]
   * Archive and Retrieval Log [IG01b]
   * Archive Box Label [IG01c]
   * Computer Use Policy [IT1]
   * Care Planning Policy [HP005]
   * Complaints Policy [Q1.16]
4. Appendices
   * Appendix 1: Document and Records Management Guidance

Appendix 1: Document and Records Management Guidance

* + 1. **Stage 1: Creation and Receipt**
  + Where records contain person identifiable data it is a legal requirement that such data be stored and processed securely.

**Good record keeping:**

1. Should prevent record duplication. Colleagues must check that a record has not already been started prior to initiating a new document.
2. Requires information to be recorded at the same time an event has occurred, or as soon as possible afterwards.

**Colleagues must:**

1. Make sure their handwriting is legible when making entries on paper records.
2. Make sure records are factual and relevant as the individual has the right gain access to their records via a Subject Access Request under the Data Protection Act.
3. Not ‘redact’ Microsoft Word documents electronically by using the black highlight text tool and provide the electronic file as a Word or PDF file, as this process is reversible. Contact the DPO for advice.
   * 1. **Stage 2: Distribution**
4. When emails, including encrypted attachments, are received containing personal or sensitive information, they must be stored securely on receipt and completely deleted from the email system when no longer needed.
5. Where email is used to send personal information, do not include person identifiable information in the subject heading.
   * 1. **Stage 3: Use (Active Phase)**

**Records Security: Work Base, Home Working, Mobile Working**

**Colleagues must:**

1. Securely save all person identifiable data or commercially sensitive data (see also IT1).
2. Not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of MHA.
3. Use portable media in accordance with MHA’s IT policies and procedures. Ideally, person sensitive data must not be stored on any portable media, however if there is no other option, colleagues must make sure this data is securely stored and deleted once transferred to a secure area folder.
4. Make sure they collect all documents immediately after printing when printing paper records, especially sensitive documents.
5. Make sure security measures and precautions are in place, by the sender and receiver, when transferring data.
6. Never leave a computer screen open when unattended - always lock it using the keys:

* <Control> + <Alt> + <Delete> then click on ‘Lock This Computer,’ or
* <Windows Key> + <L>

**Scanning**

1. For reasons such as business efficiency and / or to address problems with storage space, colleagues may consider the option of scanning paper records into electronic format. Large scale scanning can be a very expensive option and must only be undertaken after approval by a Regional Director.
2. Colleagues involved in scanning paper records into electronic format with the purpose of discarding the original paper file, must ensure the security of the scanned files.

**Record Access**

1. All requests for records containing personal data must be logged with the Data Protection Officer.

**Record Disclosure**

1. Not all records can be disclosed. Contact the DPO before disclosing records.
2. There are legal conditions that do not require consent for records to share records. Contact the DPO for further information.
3. All disclosures of records must be logged and processed by the Data Protection Officer to ensure appropriate data protection requirements and exemptions are met.
   * 1. **Stage 4: Maintenance (Archiving)**

**External Archiving**

1. Only use external storage solutions approved by Procurement.
2. Paper file storage must be kept dry, be safe from unauthorised access and meet fire regulations.
3. Information Asset Owners (IAOs) must make sure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of MHA.
   * 1. **Stage 5: Disposition / Disposal**

**Record Retention Schedule**

1. Records must be destroyed in accordance with MHA’s retention schedule. It can be a personal criminal offence to destroy information requested under the UK GDPR or the Data Protection Act.
2. The recommended retention periods shown on the retention schedule apply to the official or master copy of the records. Any duplicates or local copies made for working purposes must only be kept for as short a period of time as possible – although duplication should be avoided unless absolutely necessary.

**Records with a Legal Hold**

1. Colleagues who become aware that records (electronic or paper) may be needed for a legal case, insurance claim, investigation or enquiry must immediately notify their line manager, who in turn must escalate the notification to the appropriate Director. A Legal Hold may need placing on these records.
2. Details of the records which have been placed on a Legal Hold must be logged.
3. When a Legal Hold is terminated, the records hold must be retained or destroyed in accordance with the applicable retention period.

1. Version Control

| Version | Version Date | Revision Description / Summary of Changes | Author and Review Panel | Next Review Date |
| --- | --- | --- | --- | --- |
| 2.00 | May 2024 | Review and merging of IG001, IG006, IG007, IG008, IG010 and appendices | Author  Data Protection Officer  Review Panel  Standards and Policy Manager | May 2027 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |