NATIONAL MUSEUMS NI

# Data Retention and Disposal Schedule

| Ver | Created By | Approved By | Approval Date | Scheduled Revision | Creation Date |
|---|---|---|---|---|---|
| 1.0 | David Milnes | | | | 11/11/2024 |

# Contents

## Introduction:

The retention schedule aims to support the development of greater control over the records created by National Museums NI business data. Its primary goal is to ensure compliance with legal and regulatory requirements, protect sensitive information, and optimize storage resources.

## Roles & Responsibilities

All National Museums NI staff are responsible for managing the information they create and receive as part of their normal daily business activities and should familiarise themselves with the Retention and Disposal Schedule.

Specific records management responsibilities are also allocated to individual staff members and various committees and boards across our corporate structure, as detailed in our Information Risk Management Network. The following roles have additional responsibilities around retention and disposal:

- **Information Asset Owners (IAO):** IAOs ensure that all assets under their control are following retention schedule rules. They have ownership of the assets and are therefore responsible for ensuring adherence to the Retention and Disposal Schedule. IAOs are responsible for authorising the destruction of information when required.
- **Information Asset Managers (IAM):** IAMs assist the IAOs in their role and are operationally responsible for the upkeep of information assets, including adherence to the Retention and Disposal Schedule.
- **Local Information Management Officer (LIMO):** LIMO monitor compliance with the retention schedule, whilst encouraging and working with staff to ensure ongoing conformity. Alongside this, the LIMO reports to the IAM and IAO on compliance with the schedule within their team. They also need to implement any changes required to the schedule in accordance with ICO procedure and work to improve compliance with the schedule where needed.
- **Local Asset Administrator (LAA):** LAA work with staff directly to ensure the retention schedule is adhered to, undertaking some work disposing of information and recording disposal where needed. The LIMO is likely to delegate instructions to the LAA to assist in improving compliance with the schedule.

## Scope:

This policy schedule applies to all employees, contractors, and third-party service providers who have access to or handle corporate data.

## Definitions:

- **Corporate Data:** Any information created, received, or transmitted by the company, including but not limited to:

    - Electronic information (e.g., o356 data, emails, documents, databases, network devices, backup systems)
    - Physical records (e.g., paper documents, files, reports)
    - Personal information (e.g., customer data, employee records)
    - Intellectual property (e.g., patents, trademarks)
- **Retention Period:** The length of time that National Museums NI must retain data.
- **Disposal:** The permanent deletion or destruction of National Museums NI data.

## Retention Schedule:

The following retention schedule outlines the maximum retention periods for various types of data. Specific retention periods may vary depending on legal requirements, industry standards, and business needs.

Master copies of records should be retained for the periods specified in the retention table. These are typically the official versions kept for regulatory or business purposes. If a master copy is stored elsewhere within National Museums NI, there's no need to duplicate it. Copies of records should never be retained longer than the retention period for their corresponding master copy.

## Data Disposal Procedures:

- **Secure Destruction:** All physical records must be destroyed using a secure method, such as shredding or pulping.
- **Electronic Destruction:** Electronic data should be deleted using secure methods that prevent recovery.
- **Certification:** A certification process should be in place to verify that data and hardware has been disposed of properly.

## Data Retention and Access Controls:

- **Access Controls:** Access to organisational data should be restricted to authorized personnel on a need-to-know basis.
- **Regular Reviews:** The data retention schedule and procedures should be reviewed regularly to ensure compliance with changing legal requirements and industry standards.
- **Data Classification:** All data should be classified based on its sensitivity and value to the organization. This will help determine appropriate retention periods and security measures.

## Compliance with Legal and Regulatory Requirements:

There are various pieces of legislation which outline retention requirements. These include, but are not limited to:

- Freedom of Information Act 2000 – including the Code of Practice Section 46 (FOIA)
- The UK General Data Protection Regulations (the UK GDPR)
- Data Protection Act 2018 (DPA 18)
- Public Records Act 1958
- Limitation Act 1980
- Inquiries Act 2005

## Data Breach Response:

In the event of a data breach, National Museums NI must promptly investigate the incident in line with the procedure outlined in the Data Protection Policy (Appendix B), by notifying affected individuals and authorities as required by law, and take steps to prevent future breaches.

For further information visit the National Museums NI privacy statement (https://www.nationalmuseumsni.org/privacy-statement).

## Employee Awareness and Training:

All employees are required to familiarize themselves with the organization's comprehensive data retention schedule. To ensure compliance and prevent unauthorized data breaches, employees must undergo mandatory training sessions that cover the following key aspects:

- **Data Classification:** Understanding the different levels of data sensitivity and the appropriate security measures required for each.
- **Data Access Controls:** Implementing robust access controls to restrict data access to authorized personnel only.
- **Data Storage and Retention:** Adhering to the prescribed retention periods for various data types to minimize storage costs and mitigate risks.
- **Data Disposal:** Implementing secure methods for disposing of sensitive data to prevent unauthorized access or misuse.

By providing employees with a thorough understanding of the data retention schedule and equipping them with the necessary skills to handle data appropriately, the organization can significantly reduce the risk of data breaches and maintain compliance with relevant regulations.

## Review and Updates:

The data retention schedule should be reviewed annually and updated as needed to reflect changes in legal requirements, industry standards, and business practices.

By implementing a comprehensive data retention schedule, National Museums NI can protect sensitive information, reduce the risk of data breaches, and ensure compliance with legal and regulatory requirements.

## Data Retention Schedule:

| Personal Data Processing | Reason to retain | Retention period |
|---|---|---|
| **ICT** | | |
| Staff Account & user drives | Legitimate interest | 90 days after staff member leaves the organisation. OneDrive recycle bin 30 days after. |
| Databases | Legal obligation | Financial information retained for seven years |
| Backup systems | Legitimate interest | Disk to Disk - Overwritten 7 days<br>Disk to Tape – 7 years<br>Disk to Cloud - 7 years |
| Photographs, Video & Audio | Legitimate interest | 5 years |
| Project Storage (online & on-prem) – Covered by project lifespan | Legitimate interest | As per project end date |
| Security systems | Legitimate interest | 2 years |
| Help desk | Legitimate interest | 5 years |
| Redundant data drives | Legitimate interest | Secure disposal / Data erasure within 90 days |
| Profile data | Legitimate interest | 1 year |
| Network monitoring – Public | Legitimate interest | All data anonymised, kept under consent or cleared within 30 days |
| Network monitoring – Staff | Legal obligation | 3 years |
| **Operations** | | |
| Health & Safety - Visitors | Legal obligation | Visitors - 3 years<br>Customers – 3 years<br>Staff - As long as necessary |
| Contractors - Supplier Information | Contractual Basis | 3 years post contract end date |
| CCTV Footage | Legal obligation | Footage will be kept for a maximum of one year with reviews every 3 months to consider if still required. Video footage is generally overwritten every three weeks. |
| Notice Prohibiting Entry (users excluded from entry) | Legitimate interest | Data will be retained for the exclusion period plus and additional probation period. If the exclusion period is 6 months, the data will be held for a further 6 months. |

| | | |
|---|---|---|
| Sign-in App – Suppliers / Visitors / Staff / Third-Parties / Contractors | Legitimate interest | Employees – Unlimited (Employee details managed by our Active Directory).<br><br>Contractors & 3rd Parties – Data will be retained for 2 years. |
| **Finance & Governance** | | |
| Supplier data | Contractual Basis | 6 years from the end of the last company financial year they relate to |
| Trustee personal details | Legitimate interest | 6 years post the date their term ends |
| Employee register of interests | Legitimate interest | 6 years post leaving date |
| Membership – HMRC gift aid donations | Legal obligation | 6 years from the end of the last company financial year they relate to |
| Customer and transactional data. This relates to a range of online and in person transactions, including museum tickets, event tickets, and guidebooks. | Legal obligation | 6 years from the end of the last company financial year they relate to |
| Pensions data | Legal obligation | The museum has a legal obligation to retain employee data for the purposes of pensions |
| **Human Resources & Organisational Development** | | |
| Employee data | Legal obligation | 6 years |
| Job applications | Legitimate interest | 1 year |
| Volunteer data | Legitimate interest | 3 years |
| **Collections Services** | | |
| Object Information | Legitimate interest | Unlimited - Article 6(1)(e) - public interest |
| Donors | Legitimate interest | Unlimited - Article 6(1)(e) - public interest |
| finders and landowner details and statements | Legal obligation | Article 6(1)(c) - legal obligation |
| Lender information – Lenders & couriers | Contractual basis | 7 years |
| Picture Library Information - customers | Legal obligation | 1 year |
| **Curatorial** | | |
| Artist information | Legitimate interest | Unlimited - Article 6(1)(e) - public interest |
| General Enquiries – data stored securely in the museum's audience enquiry database. | Legitimate interest | 2 years |
| Education bookings - Schools, Teachers | Contractual Basis | 7 years |
| **Visitor Services** | | |
| Visitor information | Contractual Basis | 1 year |

| | | |
|---|---|---|
| Commercial clients | Contractual Basis | 7 years |
| Members data | Legitimate interest | National Museums NI will retain personal data for administrative purposes for up to 2 years from the date of purchasing their membership. |
| Enquiries made to the museum | Legitimate interest | 2 years |
| Complaints/compliments – data stored securely in the museum's Visitor Feedback database.<br>Where the complaint comes in through social media, the Communications Team will delete personal contact details once the complaint/compliment has been passed on to the Director's Office who manage Visitor Feedback. | Legitimate interest | 2 years |
| Group bookings – Community groups, group bookings, visitors | Contractual Basis | 7 years |
| **Audience Development** | | |
| Marketing data relating to individuals who have signed up to receive marketing information, e.g. e-newsletter or direct mail, and to be kept informed of events/news. We are required by GDPR to contact all the individuals held in this database to ensure they 'opt in' to receiving news in future. | Contractual Basis | 3/5/7 years post visit.<br>Once opted in, we will continue to communicate with them unless they opt out. |
| Exit surveys | Legitimate interest | 2 years following the completion of the project. |
| Social media platforms & management tools | Legitimate interest | 2 years |
| Social media / imagery | Consent (Explicit) | 3/5/7 years post visit |
| Online tracking services | Legitimate interest | Visitors must opt-in to enable tracking services. No personal data is captured or retained. |
| Analytical platforms | Legitimate interest | 14 Months as per GA4 standard retention period. |
| **CEDAR** | | |
| Data recording platform | Legal obligation | Personal data relating to uploaded records. |
| **Partners & Associates** | | |
| Friends of the Museum – Database is held by the Friends of the museum (a separately constituted charity), who have their own privacy policy and systems. | Legitimate interest | One year following the date of the expiry of the membership. Information is held on a database is held securely and in accordance with GDPR. The data is shared between the Friends and the museum – so we can for example send Friends a magazine and fulfil contractual agreements to the membership. |
| Community participation projects | Legitimate interest | 2 years following the completion of the project. |
| Catering partners | Legitimate interest | Access to corporate events & wedding information. One year following the completion of the event. |

| | | |
|---|---|---|
| Research partner | Legitimate interest | Data anonymised to provide general insights around experience and audience. |
| Retail partners | Legitimate interest | Customer and transactional data captured during online transactions. |
| Retail EPoS partner | Legitimate interest | Direct access to enable support of retail operational systems. |
| ICT partners | Legitimate interest | 2 years following the completion of the project. |
| **Microsoft Teams** | | |
| One-to-one or quick chat messages | Legitimate interest | Deleted automatically after 90 days |
| Messages between supplies / partners | Legitim ate interest | Exempt from auto deletion |
| Teams meetings | Legitimate interest | 2 years |

## Compliance & Assurance:

The Data Protection Officer will lead an audit of compliance with the Data Retention Schedule on annual basis.

From time to time and as appropriate Internal Audit will review compliance with all aspects of Data Protection and Retention Policy and Procedures.

For any support with compliance please contact the Information Officer in the first instance.