Data Protection Policy

Document Control

Policy owner: Director
Approved by: Board of Trustees
Effective from: 01/04/2026
Review date: 01/04/2029
Version: 1.0

1. Purpose

The Natural Sciences Museum, Sheffield ("NSM") is committed to protecting personal data and handling it lawfully, fairly, securely and transparently.

This policy sets out how NSM will comply with applicable data protection law when processing personal data relating to trustees, staff, volunteers, visitors, researchers, donors, members, contractors, suppliers, students, event attendees, supporters, and other individuals connected with NSM.

Its purpose is to:

- protect the rights and freedoms of individuals;
- support lawful and responsible museum operations;
- reduce the risk of data loss, misuse, breach or unlawful disclosure;
- ensure accountability for data protection compliance; and
- support public trust in NSM's governance and stewardship.

2. Scope

This policy applies to:

- Trustees;
- the Director;
- Heads of Department;
- staff;

- volunteers, interns and students;
- contractors, consultants and agency workers;
- researchers and formal visitors working with NSM systems, records or collections information; and
- anyone else processing personal data on behalf of NSM.

It applies to personal data processed by NSM in any format, including:

- paper records;
- emails and correspondence;
- databases and collections systems;
- HR, volunteer and trustee records;
- donor, supporter and membership records;
- education and event records;
- CCTV or other image-based monitoring;
- websites, apps and digital services;
- audio, video and photographs; and
- archived records and research datasets containing personal data.

3. Policy Statement

NSM will process personal data only where there is a lawful basis to do so and will do so in accordance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. Those principles sit at the heart of the UK GDPR, and the accountability principle requires organisations to take responsibility for compliance and be able to demonstrate it.

4. Governance and Authority

NSM's authority structure is:

Trustees → Director → Heads of Department → staff

4.1 Trustees

The Trustees have overall responsibility for ensuring that NSM maintains appropriate data protection governance and oversight.

4.2 Director

The Director is responsible for implementing this policy, ensuring that suitable controls are in place, and escalating serious risks or incidents to the Trustees where appropriate.

4.3 Data Protection Lead

NSM will appoint a Data Protection Lead to coordinate compliance, maintain policies and records, support training, advise on risk, and coordinate data protection incidents and rights requests.

If NSM is ever legally required to appoint a Data Protection Officer (DPO), it will do so and ensure that the role is independent and properly resourced. ICO guidance states that some organisations are required to appoint a DPO, but not all.

4.4 Heads of Department

Heads of Department are responsible for ensuring compliance within their departments, including local procedures, secure handling, record-keeping, and escalation of risks and incidents.

4.5 Staff and others

Everyone covered by this policy must handle personal data in accordance with this policy, related procedures, and any instructions issued by NSM.

5. Definitions

For the purposes of this policy:

Personal data means any information relating to an identified or identifiable living individual. The Data Protection Act 2018 defines personal data in this way.

Special category data means personal data requiring extra protection, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, or data concerning a person's sex life or sexual orientation. The ICO confirms that such data requires both a lawful basis under Article 6 and a separate condition under Article 9.

Criminal offence data means personal data relating to criminal convictions, offences, allegations or related security measures, which requires additional legal conditions.

Processing means any use of personal data, including collection, storage, consultation, adaptation, disclosure, deletion or destruction.

Controller means the organisation that decides why and how personal data is processed.

Processor means a person or organisation processing personal data on behalf of a controller.

6. Types of Personal Data Processed by NSM

NSM may process personal data in connection with:

- employment, volunteering and trustee administration;
- payroll, pensions and finance;
- recruitment and safeguarding;
- memberships, donations, patronage and fundraising;
- visitor services, ticketing, retail and events;
- education and learning activities;
- research access, enquiries and specimen or collections use;
- collections records, archives and museum history where personal data is present;
- supplier and contractor management;
- security, access control and CCTV;
- website, digital engagement and communications; and
- legal, regulatory and insurance matters.

Some of this information may include special category data, criminal offence data, children's data or archived personal data requiring heightened care.

7. Lawful Basis

NSM will identify and document an appropriate lawful basis for each processing activity before processing begins.

Depending on the activity, lawful bases may include:

- consent;
- contract;
- legal obligation;
- vital interests;
- legitimate interests; and
- in limited cases, public task where that basis is genuinely available in law.

The ICO states that every processing activity requires a lawful basis under Article 6, and that if special category data or criminal offence data is involved, additional conditions must also be identified and documented.

NSM will not rely on consent where another lawful basis is more appropriate or where consent cannot be freely given or easily withdrawn.

8. Special Category and Criminal Offence Data

NSM will process special category data and criminal offence data only where strictly necessary, proportionate and supported by the required legal conditions.

This may arise, for example, in relation to:

- HR and occupational health matters;
- accessibility and reasonable adjustments;
- safeguarding;
- equality monitoring;
- certain research activities;
- security and incident management; or
- legal claims and compliance matters.

Where required by law, NSM will maintain any appropriate policy document and additional safeguards needed for such processing. The ICO states that special category processing requires both an Article 6 basis and an Article 9 condition, and the Data Protection Act 2018

provides additional conditions in Schedule 1 for special category and criminal offence data.

9. Transparency and Privacy Information

NSM will provide privacy information to individuals in a concise, transparent, intelligible and accessible form, using clear language.

Privacy information will explain, as appropriate:

- who NSM is;
- why personal data is collected and used;
- the lawful basis relied on;
- who data may be shared with;
- retention periods or criteria;
- individual rights;
- how to complain; and
- where relevant, whether data will be transferred outside the UK.

The ICO states that the right to be informed is a key transparency requirement and that privacy information should normally be provided at the time personal data is collected.

10. Individual Rights

NSM will respect individuals' rights under data protection law, including the rights to:

- be informed;
- access their personal data;
- rectification;
- erasure, where applicable;
- restriction of processing;
- data portability, where applicable;
- object; and
- not be subject to unlawful solely automated decision-making.

Subject access requests and other rights requests will be handled promptly and in accordance with law. The ICO states that organisations must respond to a valid subject access request without undue delay and within one month, with a possible extension of up to two further months where the request is complex or numerous.

Where NSM relies on an exemption or restriction, this must be lawful, necessary and documented.

11. Research, Archives and Collections-Related Data

As a museum, NSM may process personal data for archiving in the public interest, scientific or historical research, and related collections documentation purposes.

Where NSM relies on the research or archiving framework, it will do so only with appropriate safeguards and only where the legal conditions are met. NSM recognises that certain exemptions and adaptations may apply to research- or archiving-related processing, but only to the extent permitted by the UK GDPR and the Data Protection Act 2018. The ICO explains that the UK GDPR and DPA 2018 contain specific provisions for research and archiving, including exemptions in Schedule 2 paragraphs 27 and 28 and adaptations to purpose limitation and storage limitation where the legal conditions are met.

NSM will not assume that all collections or historical material is exempt from normal data protection obligations.

12. Data Minimisation, Accuracy and Retention

NSM will collect only the personal data it needs for specified purposes and will keep it accurate and up to date where necessary.

Personal data will not be kept for longer than necessary, unless lawful retention is justified for archiving, research, legal, regulatory or other legitimate reasons. The ICO states that the storage limitation principle requires personal data to be kept no longer than necessary, although data may be retained for archiving in the public interest, scientific or historical research, or statistical purposes subject to safeguards.

NSM will maintain retention rules or schedules appropriate to its operations and records.

13. Security and Confidentiality

NSM will protect personal data using measures appropriate to the nature, sensitivity and risk of the data concerned.

These may include:

- access controls and least-privilege access;
- secure passwords and authentication;
- encryption where appropriate;
- secure storage and transmission;
- confidentiality obligations;
- records management controls;
- secure disposal;
- staff training; and
- incident logging and review.

The UK GDPR principle of integrity and confidentiality requires appropriate security, and the accountability principle requires NSM to be able to demonstrate those controls.

14. Records of Processing and Accountability

NSM will maintain records of its processing activities and other documentation necessary to demonstrate compliance.

This may include:

- records of processing activities;
- lawful basis records;
- privacy notices;
- retention schedules;
- consent records where relevant;
- processor contracts;
- DPIAs;
- breach logs; and
- training and policy records.

The ICO states that most organisations must document their processing to some extent, that controllers need records of processing activities, and that accountability also requires organisations to keep records of matters such as consent and personal data breaches.

15. Data Sharing and Processors

Where NSM shares personal data with third parties, it will do so only where there is a lawful basis, a clear purpose, and appropriate safeguards.

Where a third party processes personal data on NSM's behalf, NSM will ensure that a compliant written contract is in place. The ICO states that Article 28 requires a binding contract with processors and that it must include specified protections, including confidentiality and controls over sub-processors.

NSM will also define whether it is acting as controller, joint controller or processor in any shared-data arrangement.

16. International Transfers

NSM will not transfer personal data outside the UK unless it has identified a lawful transfer mechanism and carried out the required assessment.

Where required, NSM will complete a transfer risk assessment or equivalent data protection test and put suitable contractual or other safeguards in place. The ICO's January 2026 international transfer guidance explains that restricted transfers must be assessed and that a transfer risk assessment remains part of compliance, even though the legislation now refers to a "data protection test".

17. Data Protection Impact Assessments

NSM will carry out a Data Protection Impact Assessment (DPIA) before beginning processing that is likely to result in a high risk to the rights and freedoms of individuals.

High-risk processing may include, for example:

- large-scale use of special category data;
- new technologies;
- extensive monitoring or CCTV use;
- major data-sharing arrangements; or
- new systems or projects involving sensitive or vulnerable groups.

The ICO states that a DPIA is a legal requirement where processing is likely to result in a high risk and that it should begin early in the life of a project.

18. Personal Data Breaches

Any actual, suspected or potential personal data breach must be reported internally without delay.

NSM will investigate, contain, assess and document breaches, and will notify the ICO and affected individuals where required by law. The ICO states that notifiable personal data breaches must be reported without undue delay and no later than 72 hours after the organisation becomes aware of them, and that organisations should keep a breach log even if a breach is ultimately not reported.

19. Marketing, Fundraising and Electronic Communications

NSM will conduct fundraising, supporter engagement and direct marketing in a lawful and respectful way.

Where personal data is used for fundraising or marketing, NSM will comply with the UK GDPR and the Privacy and Electronic Communications Regulations 2003 (“PECR”), including rules on email, text, telephone and online marketing where applicable. The ICO states that direct marketing includes promoting an organisation’s aims and ideals, including fundraising and campaigning, and that PECR restricts unsolicited electronic marketing with stricter rules for individuals than for companies.

NSM will maintain clear opt-out and suppression arrangements where required.

20. CCTV, Photography and Monitoring

Where NSM uses CCTV, body-worn cameras, access-control imagery or similar monitoring tools, it will do so only for legitimate purposes such as security, safety, incident investigation or protection of collections and premises.

Such processing must be proportionate, supported by appropriate signage or privacy information, and reviewed regularly. The ICO's surveillance guidance states that organisations must take a data protection by design and default approach and assess whether a DPIA is required, including for monitoring publicly accessible places on a large scale or monitoring workers.

21. Data Protection Fee and Registration

NSM will assess whether it is required to pay the ICO data protection fee and, if so, will maintain payment and registration as required.

The ICO states that organisations processing personal data as controllers generally need to pay a fee unless exempt, and that charities not otherwise exempt are liable only for the Tier 1 fee.

22. Training and Awareness

NSM will provide data protection awareness and training appropriate to role and risk.

Additional training may be required for those handling:

- HR or safeguarding data;
- donor and supporter records;
- CCTV and security systems;
- research and archival material containing personal data;
- children's data;
- sensitive complaints or incident files; or
- supplier or processor contracts.

23. Non-Compliance

Failure to comply with this policy may result in:

- withdrawal of access to systems or records;
- corrective action or retraining;
- disciplinary action;
- termination of volunteer, contractor or researcher access;
- referral to the Director or Trustees; or
- referral to the ICO or other authority where required.

24. Review

This policy takes effect on 01/04/2026 and will be reviewed by 01/04/2029, or earlier if required by changes in law, ICO guidance, organisational structure, technology, or operational risk.