Data Protection Policy

1. Scope

1.1. This policy sets out the Natural History Museum's commitment to data protection legislation (meaning any UK Data Protection Act in force from time to time, and the General Data Protection Regulation) and good practice in handling personal data. It is intended primarily as an internal document, which may be made available publicly, complementing the external privacy notice on the Museum website (www.nhm.ac.uk/privacy-notice).

1.2. The Museum collects and uses personal details about customers, visitors, donors and patrons, current, past and prospective employees, suppliers, clients and other contacts as part of our work, in order to provide or improve services, administer contracts of employment, encourage and administer donations and to comply with the legal requirements of government departments and others. However, it is recorded or used, whether on paper, electronically, or in any other medium, this data must be dealt with properly.

1.3. This policy applies to all personal data obtained, held and used by the Natural History Museum. This may be factual information such as names and addresses, or expressions of opinion, images or any other recorded information that can identify or tell something of significance about a living individual.

1.4. This policy applies to all staff who collect and/or use personal data in the course of their work. Separate guidance (including an intranet site) provides more detailed information for staff on how to comply with the requirements of this policy.

2. Background

2.1. Data protection legislation provides a framework for organisations to ensure that personal data is handled properly, and gives individuals important rights in relation to their personal information, including being able to find out what is held about them.

2.2. Data protection legislation applies to any processing of personal data.

2.2.1 'Processing' encompasses almost anything that can be done to data, including (but not exclusively) obtaining, organisation, use, retrieval, consultation, disclosure and destruction. All processing must be justified under one of the six lawful bases identified in the GDPR.

2.2.2 'Personal data' means data which relate to a living individual ('data subject') who can be directly or indirectly identified, in particular by reference to an identifier such as their name, ID number, location data, email address or online identifier (e.g. IP addresses and cookies).

2.3. The GDPR sets out a series of principles on the handling of personal data with which organisations must comply. Personal data shall be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for archives, scientific/historical research and statistics) ('purpose limitation')
- adequate, relevant and limited to what is necessary for the purpose ('data minimisation')
- accurate and, where necessary, kept up to date ('accuracy')
- kept in a form which permits identification for no longer than necessary for the purpose for which the data are processed (with exceptions for archives, scientific/historical research and statistics) ('storage limitation')
- 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 ('integrity and confidentiality')

2.4. Data subjects have the right to be informed about the collection and use of their data, the rights of rectification and erasure, the right to restrict or object to processing, the right to data portability and the right not to be subject to a decision based on automated processing.

2.5. Separate from but complementary to data protection legislation, the Privacy and Electronic Communications Regulations require particular measures to be in place when collecting and using personal data electronically. Two key areas relate to the use of cookies on websites, and the requirement to obtain a positive indication of consent from data subjects prior to direct marketing – encompassing both promotional activities and fundraising – by electronic means (email/telephone/SMS).

3. Statements

3.1. The Natural History Museum is committed to compliance with data protection legislation and takes seriously the responsibility of handling personal information. To this end the Museum endorses the data protection principles and the concept of data protection by design and default.

3.2. The Museum will ensure that all appropriate procedures and staff training are in place, so that all personal data obtained, held or used by the Museum is protected and managed in accordance with data protection legislation.

3.3. The Museum will document its use of the lawful bases for processing data in the register of data processing, and will communicate the bases used to the public via the privacy notice and fair processing statements.

3.4. The Museum will always be honest, open and proactive in communicating with people about how it intends to collect, keep, analyse and use their personal data.

3.5. The Museum will facilitate the exercise of the rights of individuals as enshrined in data protection legislation.

3.6. Data Protection Impact Assessments will be undertaken as appropriate on new projects and initiatives involving personal data and/or potentially intrusive technologies, to ensure that any potential privacy risks are identified and addressed.

3.7. Personal data will only be shared with third parties under strictly controlled conditions. Any transfer of data outside the Museum, whether within the UK or abroad, will be accompanied by a Data Processing and Confidentiality Agreement. Personal data will only be transferred outside the EU if one of the conditions as laid out in the GDPR are met, e.g. to a country on the EU approved list. If the transfer is to the USA, the recipient should be able to prove they have signed up (or are planning to sign up) to the US Department of Commerce Privacy Shield Scheme, or the EU standard contract clauses.

3.8. The Museum will implement risk-based and proportionate technical and organisational measures to ensure and demonstrate compliance with data protection legislation.

3.9. Data subject rights requests will be dealt with within 28 calendar days. The Museum reserves the right to charge for or refuse to act on a request that is manifestly unfounded or excessive.

3.10. The Museum will also comply with the requirements of the Privacy and Electronic Communications Regulations (PECR).

3.11. The Museum will operate its CCTV system and manage the automatically gathered data in accordance with the principles of data protection legislation and the Information Commissioner's CCTV Code of Practice.

4. Roles and responsibilities

4.1. The Museum as the data controller is responsible for compliance with data protection requirements, and is required to ensure and be able to demonstrate compliance with data protection legislation.

4.2. All staff are responsible for ensuring that any personal data which they collect or hold is managed in accordance with the data protection principles and that any suspected or actual personal data breach is reported immediately according to the Data Breach Reporting Procedure.

4.3. The Museum's Data Protection Officer (the Information Manager) will advise staff on how to comply with data protection legislation, monitor compliance, coordinate responses to Subject Access Requests, deal with complaints and act as the contact point with the Information Commissioner's Office. The Data Protection Officer can be contacted at dataprotection@nhm.ac.uk

4.4. The Museum's Senior Information Risk Owner (SIRO) is the Director of Finance and Corporate Services, who has overall responsibility for the Museum's management of information risk, and may give final approval or veto for projects with significant data protection/privacy issues.

Version:	2.0
Approved by:	SIRO, 26 June 2018
Contact:	Data Protection Officer
Last updated:	May 2018
Review date:	May 2019