Data Protection Policy

1 Scope

1.1 This policy sets out the Natural History Museum's commitment to the Data Protection Act 1998 and good practice in handling personal data.

1.2 The Museum collects and uses personal details about current, past and prospective employees, suppliers, clients, customers, visitors, donors 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 The Data Protection Act 1998 (DPA) 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 The DPA 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.

2.2.2 'Personal data' means data which relate to a living individual who can be identified from those data alone, or from those data and other information which is in, or likely to come into, the Museum's possession.

2.3 The DPA sets out eight Principles on the handling of personal data with which organisations must comply:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
2. It shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose/those purposes.
3. It shall be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed.
4. It shall be accurate and, where relevant, kept up to date.
5. It shall not be kept for longer than is necessary for that purpose/those purposes.
6. It shall be processed in accordance with the rights of the data subject under the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. It shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.4 Data subjects' rights include being informed whether their information is being processed by the Museum; being provided with a description of what information the Museum holds about them; preventing processing in certain circumstances; and correcting, blocking or erasing incorrect information.

2.5 Separate from but complementary to the DPA, 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/social media).

3 Statements

3.1 The Natural History Museum is committed to compliance with the Data Protection Act 1998 and takes seriously the responsibility of handling personal information. To this end the Museum endorses the Data Protection Principles and 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 the DPA.

3.2 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.

3.3 Privacy Impact Assessments will be undertaken on new projects and initiatives, particularly those involving personal data and/or potentially intrusive technologies, to ensure that any potential privacy risks are identified and addressed.

3.4 Personal data will only be shared under strictly controlled conditions. Any transfer of data outside the Museum, whether within the UK or abroad, will be accompanied by a Data Confidentiality Agreement. If personal data is to be transferred outside the EEA, countries should be 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.

3.5 Subject Access Requests will be dealt with within 40 calendar days. Usually the Museum will not make a charge for responding to a Subject Access Request, but reserves the right to charge the £10 fee allowed under the DPA if a large amount of work will be involved.

3.6 The Museum will also comply with the requirements of the Privacy and Electronic Communications Regulations.

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

4 Roles and responsibilities

4.1 The Museum's Information Compliance Officer (the Information Manager) will advise staff on how to comply with Data Protection, and coordinate responses to Subject Access Requests. The Information Compliance Officer can be contacted at dataprotection@nhm.ac.uk

4.2 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.

4.3 All staff are responsible for ensuring that any personal data which they collect or hold is managed in accordance with the Data Protection principles, including being kept securely, only shared with authorised people, and not used for any other purpose than for which it was collected.

Version: 1.3
Approved by: Corporate Services Executive, 3 May 2017
Last updated: December 2016
Review date: December 2018