SCIENCE MUSEUM GROUP

Information Management Policy

Science Museum Group, 2017

Version 1

Approved Date: 21st March 2017

Review Date: on or before 21st March 2020

INTRODUCTION

As a group of national museums, SMG has numerous assets (collections, buildings, websites, information, brand, intellectual output etc.) through which our mission is fulfilled. Museums thrive on multi-disciplinary collaboration where cross- departmental teams of specialists work together toward shared goals, accessing existing assets and creating new assets. Good management of information is fundamental to working effectively together.

Information is as important to the achievement of SMG's mission and vision as any other tangible asset. Information assets may be records, files or data in paper or digital form. To collaborate well, operate effectively and create great experiences for our audiences, information management, stewardship and access is critical.

POLICY STATEMENT

The Science Museum Group is committed to achieving a culture of compliant and effective information management in which there is a shared group-wide understanding that information is a critical asset.

SMG aims to maximise the value of the information it holds by ensuring that it is:

- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically;
- held safely and securely;
- shared appropriately and lawfully; and
- only retained as long as it is needed, then disposed of appropriately.

It is a key requirement of SMG's approach to information that it is protected from internal and external threats whether intentional or accidental. In order to achieve this aim SMG will seek to ensure that:

- information is protected against unauthorised access;
- confidentiality is clearly understood and maintained;
- regulatory and statutory requirements are met;
- information security training is provided to all staff;
- breaches of information security are investigated efficiently and effectively; and
- business continuity plans are implemented, tested and kept under review.

SMG will match information risk (and therefore sensitivity) to information security.

SMG will adopt a digital first principal for information. Primary records will be held in digital format, with residual paper records held appropriately and digitised over time as resources allow.

ROLES AND RESPONSIBILITIES

1. *Information Management Group (IMG)*

The responsibilities of the IMG are to:

- establish a single set of principles (policies and procedures) for Information Management including for classification and security;
- ensure those policies and procedures are adequate to meet regulatory and statutory compliance requirements;
- oversee management of a register of all information assets with regular assurance from information owners;
- investigate and record any incidences of information loss, ensuring corrective action is put in place;
- ensure processes for managing information are documented and disseminated; and
- seek to foster positive culture change in the area of information management, including through establishing an on-going programme of dissemination and training.

2. *Information owners*

Information owners are responsible for:

Identifying the information they hold;

Ensuring that information is captured in SMG's information asset register;

regularly reviewing the completeness and accuracy of their information;

Reporting periodically to the Information Management Group to provide assurance on how well they are managing their information;

Ensuring a clear retention schedule is in place for their information and that only relevant, high quality information is retained;

Ensuring their information is appropriately classified;

Ensuring full use is made of their information, that it is appropriately shared and understood, so that SMG benefits from all its information assets.

3. *All SMG employees and contractors*

SMG employees and contractors are responsible for:

- Familiarity with and adherence to SMG's Information Management Policy;
- Managing information with care;
- Considering the purpose of every record they create and making an active choice to keep or delete;
- Making sure all information is classified appropriately;
- Reporting any loss of sensitive information

REGULATORY FRAMEWORK

SMG's regulatory and statutory obligations include but are not limited to those set out in the:

- Public Records Act 1958 (as amended) which relates to management and retention of public records held by SMG;
- Data Protection Act 1998 which relates to how SMG holds and uses information relating to living individuals;
- Electronic Communications and Privacy Regulations 2003 which relates to how SMG uses client contact details for marketing;
- General Data Protection Regulation 2016* which updates the laws set out in the Data Protection Act 1998;
- Freedom of Information Act 2000 which relates to SMG's obligations to release information at the request of the public;
- Payment Card Industry Data Security Standard;
- all relevant Health & Safety legislation which relates to SMG's obligations around the health and safety of our staff, contractors and third parties;
- Cabinet Office guidance; and
- ISO 270001 Certification on Information Security.

*insofar as this is implemented into UK Law.

ASSOCIATED POLICIES

This policy will form part of the SMG approach to information governance, which incorporates the following policies and procedures:

- Staff Handbook;
- Staff Vetting Procedures;
- Procurement Policy;
- Information Breach Incident Response Plan;
- Disaster Recovery Plan;
- Information and Equipment Destruction Plan;
- Document/Data Retention Policy;
- Archiving Procedures;
- ICT Policy;
- Collections Information and Access Policy;
- Freedom of Information Policy;
- Data Protection Policy; and
- Access to Information Procedure.

MONITORING

Compliance with the policies and procedures laid down in this document will be monitored by the Information Management Group together with independent reviews by internal and external audit on periodic basis. The IMG will also ensure that the monitoring, revision and updating of this Policy will take place on a 5 yearly basis or sooner as the need arises.