

---

# Information Risk Policy

*This policy was approved by the Trustees on 3 December 2020 and will be reviewed no later than 2025.*

## 1. Introduction

The information the Museum holds is an asset: it improves services to the public, helps to make the Museum more efficient and has financial value. Information handling represents a significant corporate risk: any failure or breach of security may cause damage to the reputation of the Museum nationally and internationally. This policy addresses these risks and forms part of both the British Museum's information strategy and its risk management framework. It is to be read in conjunction with existing internal documentation, guidance and procedures which relate to information management and security.

## 2. Definitions

Managing information risk means taking a proportionate approach in order to ensure information is properly protected from loss or unauthorised disclosure and ensuring that information assets are exploited effectively for the benefit of the Museum and its stakeholders.

## 3. Statement of Intent

The Museum is committed to making the best use of the information it holds. It ensures that adequate safeguards are in place to keep information secure and protects the right of the individual to privacy. In managing information risk, the Museum abides by the relevant legislation and operates within the strategic information and security framework administered by the Cabinet Office. The Museum complies with the corporate governance and accountability requirements promulgated by HM Treasury and observes guidance from the Information Commissioner.

Trustees recognise the importance of having the right culture in place to underpin information security so that information risk is understood and efficiently handled.

#### **4. Responsibilities, monitoring and audit**

The Trustees own and are responsible for managing information risk. As Accounting Officer, the Director has responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. The Audit Committee reviews information risk on the basis of a report from the Senior Information Risk Owner: the Deputy Director (Operations). The Internal Controls Committee addresses information risk on a regular basis. The Annual Report and Accounts includes summary material on information risk. This covers the overall judgement provided in the Statement of Internal Control, including any information risk incidents deemed sufficiently significant for the Information Commissioner to be informed and describes actions taken to prevent recurrence. Budget holders are designated as Information Asset Owners and are required to identify what information is held, who has access to it and how and why it is processed .In certain circumstances system owners can also be designated Information Asset Owners by the Senior Information Risk Owner. Information security procedures and protocols are promulgated across the Museum so that all staff,volunteers and contractors are made aware of their responsibilities when handling information.

#### **5. Review**

This Policy may be subject to review at any time, in the light of any incident of loss or inappropriate disclosure of information and, in any case, within five years.