Security Policy

Signed off by Security and Safety Committee | March 27, 2025| Version no. 0.1

Next Review Date	*01/04/2026*	Review Frequency	*12 months*

Policy Overview

1. Policy Statement

1. Policy Statement

The V&A's Security Policy outlines our strategic goals and obligations, modelled after the Cabinet Office's Security Policy Framework (SPF).

It ensures that all aspects of our security provision complement and support each other, aiding us in achieving our strategic goals. This policy serves as a framework to guide the development of further policies, procedures, and guidance to address specific security needs. It is applicable to all our sites in the United Kingdom and includes staff, contractors, and volunteers, while they are employed by or working for the V&A.

While procedures and local guidance may vary from site to site, they must always be consistent with and supportive of this policy.

Policy Principles

1. The museum's Board of Trustees hold ultimate responsibility for security. The Chief Operating Officer is the designated senior individual charged with delivering this responsibility.
2. We all share a collective responsibility to ensure that our staff, visitors, and assets (both information and physical) are protected in a proportionate manner from illegal or malicious activities.
3. Individual departments must manage their security risks within the parameters of this policy.
4. We will share information (including personal data) confidently, knowing it is reliable, accessible, and protected.
5. We employ staff (and contractors) who inspire confidence and whose identities are verified.
6. We must maintain resilience in the face of major disruptive events and have robust plans in place to minimise damage and rapidly recover.

Policy Details

2. Governance and Security

Protective security is a risk management process designed to protect assets appropriately and proportionately to the threats, while supporting our core business, including people, buildings, collections, services, and information.

Physical, technical, and procedural controls must be balanced to achieve a security approach that meets the needs and circumstances of the V&A, as well as the employment of effective and resilient business processes to respond to, investigate, and recover from incidents, supporting these controls.

3. Security of information

We will ensure that information assets are safely and securely stored, processed, transmitted, and destroyed, whether managed within the museum or by delivery partners and suppliers. We have a legal duty to safeguard the personal data entrusted to us and must strike the right balance between enabling core business, sharing data, protecting it and the rights of data subjects.

4. Personnel Security

Personnel security measures are applied to ensure the trustworthiness, integrity, and reliability of our people.

We will use a risk management approach to determine appropriate levels of access control. These controls cannot guarantee reliability and must be supported by effective supervision and line management.

5. Physical Security and Counter Terrorism

We will establish an appropriate security posture for each of our buildings and implement effective and proportionate security controls to mitigate risks to our visitors, staff, buildings, collections, assets, information, and infrastructure to reduce the risk of physical harm or loss to an acceptable level. This includes ensuring that assets held or managed by delivery partners and third-party suppliers are adequately protected.

All our sites will maintain effective and well-tested arrangements to respond to physical security incidents, including appropriate contingency plans and the capability to implement additional security controls following a rise in threat level.