THE
NATIONAL
GALLERY

INFORMATION SYSTEMS RISK MANAGEMENT STATEMENT

THE
NATIONAL
GALLERY

www.nationalgallery.org.uk

Information Systems Risk September 2011

Policy owner: Head of IS and Project Management

Introduction

The IS Department is responsible for maintaining and securing the Gallery's information systems and ensuring that they are available to authorised users. External and internal risks are regularly reviewed, with established protective measures adjusted in the light of any new vulnerabilities identified.

Risks

- Loss or misuse of Gallery information, leading to reputational damage and potential fraud, theft or damage to data.
- Failure properly to disclose information, leading to reputational damage.
- Failure to comply with relevant legislation (e.g. Data Protection).
- Business inefficiency caused ineffective use of Information systems and data.

Policies and procedures

The Gallery plans and prioritises developments of its information systems through the Information Strategy Group, responsible for maintaining the Information Strategy and supporting the co-ordination, monitoring and delivery of IS-related projects to predefined standards.

The policy under which staff may make use of the Gallery's IS facilities is included within the contract of employment for each member of staff who are reminded from time-to-time of their obligations. These include appropriate use of the Internet, software licencing procedures, password management and data protection.

The IS Department identifies those areas of technology where staff skills may need further development, and works with the HR Department for the delivery of appropriate training, ensuring that staff are able to make effective use of their information systems. The risk of loss of specific technical skills within the IS and user departments is alleviated by nominating individuals with primary and secondary responsibilities for a key system, together with comprehensive documentation to support system configuration and administration.

Health and Safety advice is provided for all staff and contractors working on site, including the proper use of IT equipment, appropriate seating, and any additional adjustment that may be necessary to suit a particular individual.

Threats from malicious attack or accidental exposure to hazards are mitigated through the use of firewall, intrusion protection and virus checking technologies. These are kept up to date as a matter of course. Additional protection is available, as appropriate, where there may be the risk of loss or compromise of information through staff working away from the Gallery. The use of regular data network penetration tests ensure that the security measures implemented are effective.

Regular technology refresh, prioritised warranty cover and comprehensive capacity planning together ensure that systems can grow to meet new demand. Conventional commercial hardware and software applications are used, allowing the Gallery to capitalise both on external advice where necessary to ensure that effective systems are in place, and interoperability using common standards.

An appropriate level of availability is maintained by providing secure and conditioned locations for server and communications equipment. Single points of failure are minimised and layered resilience incorporated to limit the impact of equipment failure or power loss. Alert mechanisms provide early indication of problems. Offsite backup storage and recovery is in place, ensuring that key operations can continue should access to the Gallery's premises be denied. The effectiveness of this is tested regularly.

Responsibilities

The Director has overall responsibility for ensuring that records are managed responsibly within the Gallery.

The Head of IS and Project Management has responsibility for the management and integrity of systems and data.

Heads of departments are responsible for ensuring that the policy is implemented in their individual departments. They should ensure that new starters complete a minimum level of competence questionnaire.

It is the responsibility of individual members of staff to ensure that they adhere to the conditions of the contract of employment regarding appropriate use of systems and data.