

THE NATIONAL GALLERY

INFORMATION RISK MANAGEMENT STATEMENT

INFORMATION April 2011

Policy owner: Director of Operations and Administration (SIRO)

Introduction

Information can take many forms, from confidential personal information to collection archive material. It also exists in a range of formats, from databases through to emails, paper and DVD. Information includes records such as contracts, business continuity plans and correspondence, as well as documents stored on laptops, blackberries and memory sticks. This policy sets out how the Gallery manages information risk and how the effectiveness of that management is assessed.

Risks

- Loss or misuse of Gallery information, leading to reputational damage and potential fraud, theft or damage to Gallery property.
- Failure properly to disclose information, leading to reputational damage.
- Failure to comply with relevant legislation (e.g. Freedom of Information).

Policies and procedures

The National Gallery recognises the importance of effective information risk management and aims to foster a culture that values, protects and uses information for the public good.

This policy has been developed in accordance with the Gallery's existing policy on risk management, with the intention that the management of information risks should become firmly embedded within existing processes and controls.

It is the Gallery's policy to manage the day-to-day use, retention and disposal of information responsibly to minimise risk. The responsibilities below set out the structure in place to ensure information risk is effectively managed.

Assurance

Assurance means confidence that the risks identified are being managed effectively. This confidence is gained through a system of assessment, to ensure the controls over information risk management are working properly. The Gallery will place reliance on the following system of assessment:

- An annual report by information asset owners on their management of information assets each year.
- The work of the Internal Controls Committee actively to review and monitor the risk environment, and to suggest changes to the systems of controls where necessary.
- The SIRO's annual written statement to the Director.
- The work of Internal Audit to test certain key controls relating to information risk management.

Responsibilities

Gallery responsibilities

The Board of Trustees (via the Audit Committee) sets risk management standards and the risk appetite for the Gallery.

Information Risk Management Statement

The Director, as Accounting Officer, is responsible for ensuring the Gallery's information risk is assessed and mitigated to an acceptable level. This is done by establishing and maintaining a sound system of internal control, designed to respond to and manage the risks the Gallery faces.

The Director discusses information risk assessments at the Audit Committee, including any reported incidents of information loss.

The Director receives an annual written statement from the Senior Information Risk Owner ('SIRO'). This assurance enables the Director to sign the Statement of Internal Control, which contains explicit reference to the management of information risk.

The Internal Controls Committee (ICC) is responsible for providing the Director with assurance that an effective system of internal control has been maintained and operated within the Gallery. The ICC meets quarterly, and as part of their review of the Gallery's risk register, assesses risks to the confidentiality, integrity and availability of information. On an annual basis, the ICC assesses the risk environment more broadly and considers changes and developments that might impact on the Gallery's management of information risk. These assessments inform the SIRO's written statement to the Director.

Specific responsibility for managing information risk is delegated to the Director of Operations and Administration, who has the role of Senior Information Risk Owner ('SIRO'). This includes:

- Ownership of the Information Risk Policy and risk assessment set out in the risk register.
- Liaising with the ICC to ensure information risk is actively managed.
- Acting as an advocate for information risk throughout the Gallery and at board level.
- Managing any incidents of information loss or misuse as set out in the incident management procedure (Annex 1).
- Ensuring the Gallery continues to comply with minimum mandatory requirements on information risk management
- Providing written advice to the Director on the management of information risk and the content of the Statement of Internal Control relating to information risk.
- Ensuring information asset owners and staff are aware of the Gallery's policy on information risk and their responsibilities through a programme of information risk awareness training.

Heads of Department responsibilities

Heads of Department are 'information asset owners'.

Information assets are the information and information systems owned by the Gallery. This might include a system such as TMS or Raiser's Edge, or a record such as a list of names and addresses or a file of correspondence.

Information asset owners are directly accountable to the SIRO and are responsible for:

- Understanding the information assets they own, and what information is held therein.
- Ensuring the security of those assets, including minimising and formally approving any use of removable media (e.g. memory sticks and laptops).
- Monitoring use of information assets by others within the department.
- Actively reviewing whether better use could be made of the information assets held.

Information Risk Management Statement

- Responding to and logging any requests for access to that information by others.
- Understanding the incident management procedure, and ensuring this is followed in the event of any loss or misuse of information being detected.
- Understanding risks relating to the information assets held and providing an annual written assessment to the SIRO on the budget holders' assurance statement.
- Raising the profile of information risk management and fostering a culture in which consideration of information risk is embedded in day-to-day Gallery activities.

Staff responsibilities

Staff are responsible for actively considering the security and appropriateness of the information they use and retain. This includes:

- Ensuring the security and proper use of passwords.
- Ensuring sensitive information is securely stored.
- Managing records so that Gallery systems contain only relevant, up-to-date and appropriate material.
- Minimising the necessity to remove any information from the Gallery and seeking permission for the use of remote media such as laptops or memory sticks.
- Bringing concerns about information risk to the attention of department head or other senior manager.
- Reporting any loss of information or information asset immediately, to department head or other senior manager.
- Ensuring information is appropriately and securely destroyed as soon as it becomes superfluous.

Related Policies

This policy sets out the Gallery's overall policy with respect to the management of information risk, but it is supported by more detailed policy statements as follows:

- Data Protection Policy.
- Freedom of Information Policy.
- Electronic Communications Policy.
- Use and protection of Collection Information Policy.
- Laptop / Mobile Device Security Policy.
- Records Management Policy.

These policies are available to all staff on the intranet (through the document library).

Information Risk Policy: Annex 1

Incident management procedure

In the event of loss or suspected loss of information or information assets, the following procedure should be followed:

- The incident (or suspected incident) should be reported immediately to your department head and the SIRO (being the Director of Operations).
- The SIRO will lead an investigation to establish the circumstances of the incident, the extent of any loss and the implications of that loss in terms of reputational and financial risk.
- The SIRO should make an initial assessment of the significance of the loss, and where appropriate inform the Director.
- Where the SIRO judges that an independent investigation is required, for example in the event of a significant incident or where the circumstances are particularly complex, Internal Audit may be asked to lead a more thorough investigation, which will involve interviewing staff or third parties involved.
- In the event that the SIRO is directly involved in the loss of information, another member of the Planning Group should be asked to lead the investigation.
- Where an incident has occurred through failure to apply Gallery policy with respect to information management, the Head of HR may be consulted and disciplinary action may be taken, in accordance with guidelines set out in the Staff Handbook.
- A report will be produced by the SIRO or Internal Audit, setting out the circumstances, extent and implications of the incident, together with recommendations for preventing any subsequent similar incident, where relevant.
- The incident report should be copied to the Internal Controls Committee, to inform their quarterly assessment of information risk management.
- The SIRO will judge whether the incident constitutes a significant actual or potential loss of personal data, which should be shared with the Audit Committee, DCMS, the NAO, the Information Commissioner and the Cabinet Office, and where this is the case will ensure that the appropriate report is made.
- The SIRO will take action to ensure lessons learned from the incident are applied to existing policies and practices. This might include implementing changes to the existing system of controls, increasing awareness of information risk, or disseminating lessons learned where there may be implications for the organisation as a whole.