

THE NATIONAL GALLERY

LAPTOP / MOBILE DEVICE RISK MANAGEMENT STATEMENT

LAPTOP / MOBILE DEVICE POLICY

Policy owner: Head of IS and Project Management

Introduction

Laptop computers and mobile devices, together with their data, are becoming an increasingly common target for thieves and the National Gallery is keen to protect all its assets and the information these assets might hold.

Risks

- Loss or misuse of Gallery information, leading to reputational damage and potential fraud, theft or damage to data.
- Physical loss of hardware.
- Lost productivity and associated procurement, data retrieval and set-up costs.

Policies and procedures

The Gallery aims to provide its staff with the equipment necessary for them to work effectively. As appropriate, staff may be provided with a laptop, in some cases, to replace a desktop computer. The IS Department maintains a pool of laptops for those who may need a laptop on loan for shorter periods.

The Gallery may also provide its staff with other mobile devices, including telephones and PDAs. Any of these devices may contain personal information and from the perspective of physical security should be treated with the same degree of care as a more expensive laptop. This policy therefore applies equally to users of mobile devices other than laptops, and the IS Department is available to provide advice and assistance should staff require it.

Scope

This policy defines the minimum standard required to minimise the security risks associated with laptop computers and other mobile devices. It applies to all National Gallery IT users, e.g. staff (employees, part-time or full-time, temporary or permanent), self employed (e.g. freelancers) and contractors who use a notebook, laptop, mobile phone, PDA or other portable device owned by the Gallery. 'Laptop' is used generically in this Policy to refer to all such items.

Security risks particular to the use of laptop computers

Laptops and other portable computing devices are especially vulnerable to loss and theft. Opportunistic and organised thieves may target laptops both within the Gallery's buildings and when users are away from their offices. There is potentially increased risk when travelling, especially if individuals are in unfamiliar surroundings or concentrating on the journey itself.

Although the majority of thieves may be after the quick profit from selling the device on the black market, there is a growing number who steal laptops specifically for the sensitive data they may contain. Such information, if revealed, could cause embarrassment, loss of reputation or significant financial or commercial impact to the National Gallery.

In the Gallery environment, such sensitive information may comprise:

- Personal details, for example, of staff, lenders and donors.
- Any information that the user would wish to remain private.

- intellectual property; e.g. research notes, data and commercially sensitive information.
- Sensitive financial data.

To counter these risks, laptop security is addressed in five ways:

- User responsibility; through increased user awareness of the risks and application of a laptop security policy (this document and the associated guidelines).
- Physical security; both at the user's 'base' and when travelling.
- Access control/authentication and encryption.
- Data protection; using software and hardware based solutions.
- Tracking/recovery; particularly for devices at high risk or containing very sensitive data.

Managing the risk

Our policy is to allow staff to use these portable devices to help them conduct their work on behalf of the Gallery. However, the risks associated with this use are managed by:

- Applying technology controls (for example authenticated login, password aging and virus checking) to protect access to information on laptops.
- Restricting access so that software cannot be installed by users.
- Providing advice to help staff understand the risks of using these devices, and how they can best be mitigated.
- Requiring staff to sign a 'Laptop / Mobile Device Loan Form' to confirm that they will abide by this policy and the guidelines.

Laptop Configuration

Domain policies that are applied to desktop computers will equally apply to laptops. This includes, amongst other, the need for all users to login, a standard login message, default password aging and password protected screen saver invoked after a set period of inactivity.

Users will not usually be granted permission to install software or change laptop configurations. However, permissions may be granted to permit the configuration of wireless connectivity. Unfortunately, these additional permissions may also allow software to be installed. The guidelines will advise staff not to do this nor change other configuration settings.

To provide an additional level of protection in the event of loss, laptops have their hard disks encrypted. There are a small number of laptops used for controlling scientific and audio visual equipment that do not use disk encryption - these devices are not used to store sensitive data. Increasingly, handheld mobile devices are able to access network resources (for example, email) and staff making use of this facility are advised of the risks to information and user credentials should the mobile device be lost or compromised.

Responsibilities

The Head of IS and Project Management has a duty to monitor the risk environment and to make amendments to the policy as necessary.

Heads of departments are responsible for ensuring that the policy is implemented in their individual departments.

It is the responsibility of individual members of staff to ensure that they sign and adhere to the guidelines in the Laptop / Mobile Device Loan Form.