Mobile Device Encryption Policy

Title:	Mobile Device Encryption Policy
Status:	Approved by Information Governance Group
Last update:	2016-01-17
Last review:	-

1 Policy

All confidential data ***must*** be encrypted where stored on a mobile device. It is the user's responsibility to ensure this is in place.

–Note: Encryption is automatic for Standard Staff Desktop (SSD) laptops.

2 Why it's important

Mobile devices are easily lost or stolen. Steps must be taken so that, if this happens, confidential data are not accessible to any unauthorised person. Note that this is effectively *the law*, as the UK Information Commissioner considers organisations losing unencrypted mobile devices containing personal data to have *taken insufficient steps* to comply with the Data Protection Act. Indeed, there have been many high profile cases where insufficient steps were taken, resulting in large fines, bad publicity and serious impact on the organisation's reputation.

One way to reduce the risks is to not store confidential data on the device in the first place, and work only "across the network", with data stored on servers. This approach has a number of advantages, although in practice there are many situations where it's convenient to store data on the mobile device itself. Furthermore, even if not deliberately saving data on the mobile device, it is common for copies to be automatically "cached" on the device, stored in "temporary" folders, or "synced" from cloud storage. It is necessary to ensure that, if the device is lost or stolen, the confidential data it may contain is not accessible to any unauthorised person.

Where a laptop is protected only with a regular login password, an unauthorised person can easily bypass this. Stronger measures are required, and this is where encryption comes in.

Encryption protects data making it inaccessible to anyone who does not possess the encryption password or "key". The encryption key may look like a normal password, but cannot be bypassed as described above. (With an SSD laptop, your GUID password unlocks the encryption). If the laptop is lost or stolen, the data is inaccessible.

3 Definitions

In this policy:

- Confidential data – data classified as either Medium or High Risk (see *Information Risk Classifications*).

- Personal data – data concerning living individuals, as defined by the Data Protection Act (1998). This is a subset of confidential data. (Not all confidential data is personal – e.g exam questions prior to sitting the exam)

4 Laptops

In most cases, the easiest and most convenient way to ensure all confidential data on a laptop is encrypted is to configure *full disk encryption*. Note that full disk encryption is now available as standard for all common operating systems (e.g, Windows, macOS, Linux).

For laptops which have Standard Staff Desktop (SSD) installed since March 2016, full disk encryption is enabled automatically. Many older SSD laptops are also already encrypted. IT Services will identify any that are not, so the necessary steps can be taken.

For ***all*** other laptops, users should in the first instance, contact their local IT support, and request that full disk encryption is enabled. Alternatively, contact IT Services for help and advice. IT Services will provide information and advice to IT Teams and other users on how to encrypt different types of laptop.

As a part of this process, it is recommended that recovery keys are kept, and stored in an appropriate safe manner – see section (7).

5 Tablets / Smartphones

Tablets and smartphones are often used to perform many of the same tasks as on a laptop or desktop computer, including handling confidential data. It is ***essential*** to set a PIN (which is not easily guessable) or enable equivalent security (e.g fingerprint check or swipe pattern) to protect the device from unauthorised use.

Where a PIN or equivalent is set, many tablets and smartphones automatically encrypt their internal storage out of the box. Older devices may not incorporate encryption, and in some cases, it may not be possible to retrofit it. Such devices are not suitable for accessing confidential data.

IT Services will provide information and advice on how to secure the most common types of tablets and smartphones.

6 Alternative to encryption – use SSD Remote

In practice it’s extremely difficult to avoid confidential data being stored on a mobile device. This *can* however be avoided by using a remote desktop service, such as SSD Remote when accessing confidential data. This is especially useful for working from a personally-owned or home computer, as it avoids storing any data on the device itself, and so avoids the need to configure encryption.

7 Recovery Keys

It is recommended that information stored on a laptop or other mobile device is a "working copy", and exists elsewhere e.g. on network filestore or other supported filestore service. This is important as the device might suffer a failure at any time (e.g physical failure of a laptop hard drive). The situation is similar where encryption is enabled, however there is the additional possibility the encryption key or password might get forgotten. Although the primary recommended measure to protect against this remains ensuring an unencrypted copy of data exists on the network, it is prudent for an alternate "recovery key" to be stored somewhere safe.

For SSD laptops, IT Services makes best efforts to keep recovery keys centrally. For other laptops, College or School IT teams should implement a similar system. This can be done via a variety of methods (e.g electronically, or paper-based - simply print recovery key and keep in a safe).

Users should not see the holding of recovery keys as posing a privacy threat. Physical access to the laptop itself is required for the key to be used. The motivation is to enable IT staff to assist users who forget a password to regain access to data on their laptop, in a manner analogous to resetting a forgotten network password to regain access to email and files stored on a server.

It is possible that a small number of users may have reasons not to provide either IT Services or local IT with a recovery key for their encrypted laptop. As the primary goal of this policy is to protect the confidentiality of data, such a situation is allowed by this policy. If the user chooses to manage the encryption themselves, they must recognise that if data is not backed up elsewhere, it may not be possible to help in the event of a forgotten password.

8 Further info

For further information and advice, please contact your local IT Team, or IT Services:

IT Services
ithelpdesk@glasgow.ac.uk
Ext. 4800