PROTECTION OF INFORMATION HELD ON MOBILE DEVICES AND ENCRYPTION POLICY (V3.5)

Table of Contents

1.0 Introduction

The University of Strathclyde must ensure that certain types of information are protected from accidental release into the public domain. It must do this both for legal and regulatory purposes (particularly in relation to Data Protection legislation and guidance from the Information Commissioner), as well as to ensure the protection of the University, its staff and its students from risks such as cyber-crime. This information is generally categorised as being confidential, sensitive, personal or of commercial value. Help on determining whether you have any such information is found in the University records management document RM Guidance 7 Determining if Information is Confidential. Guidance on Data Protection in a University context can also be found here.

Ideally all such sensitive, confidential or personal information should be located securely on University provided servers and not removed or copied from those servers. When working remotely, remote web tools can be used to access file stores, Sharepoint and email securely. More information can be found at Remote Access Help Topic.

It is however recognised by the University that, increasingly, staff have to work more flexibly and from more diverse locations. This can make it necessary to access or hold sensitive, confidential or personal information on mobile devices, such as laptops, tablets or smart phones. It can also lead to information being stored on devices located in people's homes. There is also an increasing tendency for staff to wish to use devices that they own rather than devices provided by the University (known as BYOD – Bring Your Own Device). This policy covers the protection of University information in all of these circumstances.

The aim of this policy is not to make it more difficult for staff to work effectively but instead to ensure that both individuals and the University comply with legal requirements and are protected from risks such as identity theft and other forms of cyber-crime. A balance between ensuring the security of both information and individuals needs to be made with efficient and effective working.

2.0 Policy

It is the policy of the University of Strathclyde that no electronic information, owned by the University of Strathclyde, that is confidential, sensitive, personal or of commercial value should be stored in an unencrypted format anywhere other than on secure server storage provided by the University[1] or on similar secure storage facilities provided by a partner organisation.

It is recognized that this is a challenging policy and thus the following advice is provided for individual users in particular circumstances.

2.1 Advice on Complying with the Policy

2.1.1 General

- Good management information practices should be followed. See the University Records Management information for further advice.
- The holding of confidential, sensitive, personal or commercially valuable information on mobile devices should be minimised, both in terms of volume of data stored, and the amount of time it is held.
- Where possible, University services for remote access should be used rather than downloading information to hold copies of it locally.
- The inclusion of confidential, sensitive, personal or commercially valuable information on email should be minimised.
- Individuals holding information locally on PCs, laptops or tablets must ensure appropriate backups are made. These backups, if not held centrally, should be treated with the same sensitivity and security considerations as the original data.
- Any personal or sensitive information held on secure servers should be treated as transitory, and should be securely deleted as soon as it is no longer essential to hold it on that device.

2.2.2 Laptop Devices

- Laptop computers owned by the University and which hold confidential, sensitive, personal or commercially valuable information must have their data storage fully-encrypted. This includes laptop devices used with docking stations.
- Confidential, sensitive, personal or commercially valuable information owned by the University held on laptop computers not owned by the University must be encrypted.

2.2.3 Smart Phone and Tablet Devices

Smart phones and tablets providing access to information and email on the move have revolutionized working practice. However, the loss of a smart phone or tablet leaves its user at risk of becoming a victim of

cyber-crime or identity theft. Therefore the following applies to any smart phone or tablet used to access staff services provided by the University of Strathclyde regardless of who owns the device. Additionally, it is recommended for all such devices regardless of use.

- A passcode or PIN must be set up on any smart phone or tablet. That, where possible, that the passcode used is strong (i.e. contains a mixture of letters, numbers and other characters) and more than four characters. As with a bank pin avoid anything that is easily "guessable".
- That, where possible, the device is set up to wipe all information should the wrong passcode or PIN be entered sequentially 10 times.
- Delete sensitive or commercial emails once you have finished with them.
- Limit the number of emails you are syncing to your device.
- In the event of a loss or theft, change the password to all University services accessed from the devices (and it is recommended this is done for any other services that have been accessed via that device (e.g. social networking sites, online banks, online shops)).

2.2.4 USB Devices

 Data held on USB or similar devices (e.g. memory sticks, portable hard-drives) holding University owned information or otherwise sensitive data must be fully-encrypted.

2.2.5 Devices used at Home including Desk Top PCs and Portable Harddiscs

 Any information owned by the University of Strathclyde that is confidential, sensitive, personal or of commercial value stored on devices located within an individual's home (including on backup devices) must be encrypted. This can be done by encrypting part of the hard disc or by saving files created in Word, Excel, etc with an encrypting password.

2.2.6 Public Cloud-based Storage Facilities

Cloud-based storage facilities, such as Dropbox or Sky Drive, allow individuals to access and share files. In this way they are very similar to many of the remote access services provided by the University.

- Any information owned by the University of Strathclyde that is confidential, sensitive, personal or of commercial value stored in public cloud-based storage facilities must be encrypted before storing.

2.2.7 Private Secure Storage Facilities provided by Partner Organisations

From time to time, staff will be required to store information on private secure storage areas owned by partner organisations. For example when collaborating with another University or industrial partner, information may be stored on servers owned by that third party.

- It is acceptable to store any appropriate information in a private secure storage facility, be it cloud-based or otherwise, provided by a partner organisation. Individuals using such facilities are responsible for ensuring that they meet a suitable level of security to comply with all legal and commercial needs of the University and that all Data Protection Legislation is complied with prior to using the facility.

2.2.8 Social Networking Sites

No information of a confidential, sensitive, personal or commercially valuable nature belonging to the University of Strathclyde should ever be posted on a social networking site.

2.2.9 Providing information to 3rd Parties

From time to time information has to be passed to 3rd parties for legitimate business reasons. It is vital that when this occurs that the University's Data Protection Policy is followed.

2.2 Application of the Policy

This policy applies to all users of information owned by the University of Strathclyde that is of a confidential, sensitive, personal or of commercial value.

This policy only applies to information that is not in the public domain.

2.3 Action on Loss or Theft

If a University-owned mobile device (laptop, smart phone, tablet etc, or storage media) is lost or stolen this should be reported to the IT Helpdesk. If a device is lost that holds confidential, sensitive or commercially valuable information belonging to the University of Strathclyde, this should also be reported to the IT Helpdesk, regardless of who owns the device. Staff should also make appropriate enquiries in attempts to locate the device and report any theft to the appropriate authorities.

2.4 Enforcement of Policy

This policy does not form part of the formal contract of employment for staff, but it is a condition of employment or study that employees and students will abide by the rules and policies made by the University where required to do so. Any failure to follow this policy can therefore result in disciplinary proceedings.

[1] – This includes storage provided by any Faculty, Department or Directorate and while it must be securely located it could be on or off campus.