University Policy for the encryption of personal data and mission critical information held on mobile devices

Author	C Milne/Associate Chief Information Officer Information Assurance & Governance
Approved by	University ICT Strategy and Planning Group
Approval date(s)	July 2013
Review date	July 2016
Version	1.0
Document type	Policy
Activity/Task	Information Security
Keywords	Encryption
Document location	[Insert_Saved_location]
Confidentiality	NA

Version Control Table

Version Number	Purpose / Changes	Author	Date
0.1	Initial (baseline) policy proposal Circulated to encryption project team	C Milne, Associate Chief Information Officer Information Assurance & Governance	07-Jan-2013
0.2	Updated following peer review	C Milne, Associate Chief Information Officer Information Assurance & Governance	04-Feb-2013
0.3	Updated following review at University ICT Strategy & Planning Group (section 6)	C Milne, Associate Chief Information Officer Information Assurance & Governance	19-Mar-2013
0.4	Final revisions – submitted for approval – references to Full Disk Encryption removed	C Milne, Associate Chief Information Officer Information Assurance & Governance	25-Jun-2013
1.0	Approved Policy		

Table of contents

1. Introduction

Given the:

- Prevalence of mobile [ICT] devices and the relative ease in which data and information can be transferred to such equipment and then taken outwith the University campus;
- High profile media reporting of the loss/compromise of personal data and/or other information held on such devices across the public and private sectors; and
- Introduction of monetary penalties for a breach of Data Protection legislation

The encryption of laptops, portable storage devices, USB pens etc. as one step to reduce the likelihood of unauthorised data access is now normal working practice across many aspects of the public and private sectors.

Whilst the benefits and opportunities available through working with mobile devices are widely recognised and appreciated their use is not without risk to the University, its students, staff and the wider communities served by it, where:

- Individuals are likely to experience substantial harm where their personal data and/or sensitive personal data for which the University has a responsibility for protecting is compromised where those information made available to unauthorised person(s); and
- The University's operation becomes compromised and/or its ability to retain the trust of partners and other stakeholders is damaged should personal data and/or mission critical information, become available to unauthorised persons.

This Policy is part of a framework which describes the steps to be taken by the University, its staff and third-party contractors to protect personal and sensitive personal data and mission critical information from unauthorised access, where those data and/or information are encrypted as a matter of routine when those materials are placed onto a mobile device.

2. Purpose and scope

The purpose of this Policy is to provide a set of parameters which set out the conditions that must be in place and maintained where personal and/or sensitive personal data ("personal data"), for which the University is responsible for and information critical to the operation of the University ("mission critical information") are stored on and processed through mobile devices – irrespective of the ownership of the device(s) in question.

This Policy requires that:

a) Suitable encryption solutions are deployed by the University so that the confidentiality and integrity of ***all*** forms of personal data and mission critical information are not threatened or diminished in any way through the loss of and/or unauthorised access to a mobile device which contains and/or can be used to process the said data and information;

b) The University in the deployment of encryption solutions makes suitable provision so that all data and mission critical information that have been encrypted remain

accessible to the University i.e. capable of recovery without threatening the confidentiality and/or integrity of the said data and/or information; and

c) Encryption solutions are and remain accessible to end-users so that people can readily engage with and make use of encryption standards as required through this Policy.

2.1. Intended audience

This Policy applies to all members of staff of the University, to agents and third party contractors thereof who have been granted access to personal data and/or mission critical information, where they are required to or have legitimate reason to process the said information on mobile devices.

2.2. *Where this Policy applies*

This Policy will apply to all locations and instances where personal data for which the University is responsible and/or mission critical information is held on and processed through a mobile device – irrespective of the ownership of the device in use. Consequently, this Policy will apply whether working on University premises, from home or in transit.

3. Policy statement

It is University Policy that unless a legitimate and approved exemption can apply, that all personal data and mission critical information (as defined by this Policy) must be and remain encrypted, when held on a mobile device, irrespective of the ownership of that device.

The transfer of personal data and mission critical information off-campus through the use of mobile devices should be ***the exception rather than the norm***. Where possible personal data and information should remain within the protection of the University network, with off campus access being undertaken through the use of secure remote access services provided by the University.

4. Definitions

4.1. Encryption

Is the process of converting (securely encoding) data and/or information rendering it unreadable to anyone other than those with the means to access the encoded material in its original (un-coded) form.

4.2. Mobile device

Any device that can store data and/or information (in binary form), where the device by its nature and/or design is readily portable. Such devices include but are not restricted to: laptops; USB storage devices; memory cards/sticks; recordable CDs and DVDs; MP3 players, smartphones, etc.

4.3. Personal data

Is data as defined by the Data Protection Act 1998 ("the DPA"), which identifies a living individual and relates to that person in a significant biographical sense.

4.4. Sensitive personal data

Is an extension of personal data (see above) also defined by the DPA that data makes reference to characteristics of a person's life that require additional protection such as their racial and ethnic origin, political opinions, religious beliefs or belief of a similar nature, whether they are a member of a trade union, a physical or mental health condition, their sexual life, criminal offences (actual or alleged) and details of proceedings handed down in relation to an actual or alleged criminal offence.

4.5. Processing

Means obtaining, recording, transferring or holding data or information, or carrying out any operation or set of operations on the data or information.

4.6. Mission critical information

Is data or information that if lost and/or accessed by an authorised person(s) would have a significant negative impact on the University's ability to operate normally without disruption. This may include but is not restricted to information that contains personal and/or sensitive personal data, financial information, research data, clinical data, contractual information, internal audit reports.

4.7. Confidentiality

Means ensuring that data and information is accessible only to those authorised to have access.

4.8. Integrity

Means safeguarding the accuracy and completeness of data and information.

4.9. Availability

Means ensuring that authorised users have access to information and associated assets when required.

5. Relationship with existing University Policy, procedures and Regulation

This Policy provides the overall framework for the protection of personal data and mission critical information (as defined herein), when processed through mobile devices by the means of encryption. This Policy does not work in isolation. Other University policy, (published) procedures and regulation are also of relevance in providing direction and more detailed discussion. In the main, these policy areas are concerned with preserving and maintaining the confidentiality, integrity and availability of information and information systems (i.e. *Information Security*), the legal and ethical use of information

and intellectual property and the protection of the rights and freedoms of individuals. Specific items include:

- Data protection policy;
- Information security policy; and
- Password Policy

6. Encryption of mobile devices

6.1. Centrally procured mobile devices

From July 2013 all mobile devices purchased centrally (through IT Services) will be encrypted before issuance, or as business requirements dictate devices with pre-existing hardware encryption may be procured.

6.2. Locally procured mobile devices

From September 2013 all mobile devices (with no existing hardware encryption) purchased through Schools or Services will be encrypted:

- Locally by staff within the School or Service; or
- Centrally – by passing the device to the IT Service Desk; or
- By an individual member of staff - making use of self-service encryption facilities.

6.3. Privately procured mobile devices

From October 2013 all privately owned mobile devices that are intended to be used to hold and process personal data and/or mission critical information, that requires to be protected by means of encryption (as set out herein) are to be encrypted:

- Centrally – by passing the device to the IT Service Desk; or
- Locally by staff within the School or Service; or
- By an individual member of staff - making use of self-service encryption facilities.

6.4. Level of encryption to be applied

Encryption standards will be defined by IT Services via a series of policies (at the software level). These will be deployed so that all data held on a mobile device are encrypted – striking a balance between legislative, regulatory and operational requirements. Initially, the minimum standard will be the encryption of all data created via Microsoft Office applications and text [.txt] files. That minimum standard may change as circumstanced dictate.

Over time, a series of encryption standards will be developed and deployed through this Policy, each focused on addressing a particular operational requirement and/or area of risk.

6.5. Disabling encryption

It will be a breach of this Policy where encryption is disabled on a device that is being used to hold personal data and/or mission critical information that requires to be protected by means of encryption as defined by this Policy, unless the data and information are first removed i.e. irreversibly destroyed from that device.

7. Securing smartphones

Smartphones that are used to access personal data for which the University is responsible for and mission critical information are to be protected by encryption, and where that is not possible by means of password and/or pin number.

7.1. Remote destruction of personal data and mission critical information from a University smartphone

Where a University smartphone is lost or becomes compromised in any way, the University more likely than not will move to irreversibly destroy ***all*** information and data from the device in question, unless there is a low risk of harm to others and the University.

8. Protection of encryption passwords and other authentication credentials

Individuals are reminded that passwords or other forms of credentials that facilitate access to encrypted data and/or information must be managed per the framework set out in the University Password Policy (2013). In summary:

- Physical access to encrypted data and/or information is normally controlled by use of a password. On occasion other forms of authentication may be used. Such credentials are assigned to individuals or selected and created by them on the strict understanding that each person:
    - Accepts that all authentication credentials in place to access encrypted data and/or information are for their sole use;
    - Recognises that authentication credentials must not be disclosed or released in any form to any other individual. This includes University staff charged with systems administration and/or IT support functions;
    - Is responsible for taking all reasonable actions to maintain and preserve the integrity of all authentication credentials in use – in particular their nondisclosure or release in any form to any individual; and
    - Shall take sensible precautions to ensure that ICT facilities and/or data/information to which access is authenticated via username and password etc. are denied to all other persons other than the legitimate Authorised user; and
    - Recognises that they may be held liable by the University for misuse of ICT facilities and/or the compromise of encrypted personal data and/or mission critical information (or other associated actions) where the they have not taken the steps necessary to maintain the confidentiality and integrity of authentication credentials issued to, or selected and created by them.

9. The (temporary) storage of personal data and mission critical information on mobile devices

Storage of personal data and/or mission critical information on mobile devices will normally be a short term, temporary measure. In most instances those data and information must be transferred from a mobile device and held within the protection of the University network.

10. Responsibilities

10.1. Chief Information Officer ("the CIO")

- The CIO has overall responsibility for ensuring that the University maintains the capability to encrypt mobile devices meeting the encryption standards set by the external authorities referred to within this Policy.
- Management of the University Information and Communications Technology estate, by ensuring that:
    - Encryption policy standards to be deployed to devices that fall within the scope of this Policy are likely to provide sufficient protection, without threatening the performance degradation of devices;
    - The recommended standard ICT equipment remains capable of being encrypted without undue performance issues that may mean that end users may become inclined to avoid encryption and/or use of that equipment and that partial disk encryption is available for use where full encryption is not appropriate;
    - IT Services can provide a timely and effective centralised purchasing service for University approved mobile devices on behalf of staff;
    - From June 2013 all University mobile devices (procured centrally) are fully encrypted at the time of issue; and
    - Ensuring that adequate provision exists for the irreversible and certified destruction of all data and information from University mobile devices prior to the decommissioning of those devices in line with University policy and processes.

10.2. The Associate Chief Information Officer (Information Assurance & Governance) ("The ACIO-IG")

- Providing advice and guidance on University encryption standards and processes;
- Ensuring that the University has access to an appropriate range of encryption policies (at the software level);
- Promoting and fostering a wide awareness and appreciation of this Policy across the University;
- Working with others to ensure that the University Service Desk has the capacity to support all persons who are required to adhere to this Policy with any problems or issues arising from the encryption of devices and/or the recovery of data and information from encrypted devices.

10.3. Heads of School or Services

- Working to ensure that their staff are fully aware of their responsibilities as set out within this Policy – specifically that personal data and mission critical information (as defined herein) are not placed onto mobile devices irrespective of their ownership, without those devices first being encrypted as per the standards set out herein.
- Staff prior to leaving the University or before transferring to another role return University mobile devices – thereafter those devices will be recycled by IT

Services or locally within the School/Serviced ensuring that all data and/or information have been irreversibly destroyed before devices are re-encrypted.

- Wherever possible, all mobile devices are procured through central purchasing service.
- Provide reasonable assistance to IT Services with equipment audits, recalls and the monitoring of the effectiveness of this Policy.
- Inform the ACIO-IG if this Policy presents any operational challenges that may adversely impact upon their School/Service.

11. Methodology

The development of this Policy was partly informed by external benchmarking. This included a review of encryption policies from higher education institutions and public sector bodies within and outwith the UK. On conducting an initial screening exercise, it was determined that implementation of this Policy would not negatively impact on any of the individual equality strands. Therefore a full Equality Impact Assessment is not required.

12. Review

This Policy will be reviewed at regular intervals. The review period will be approved by the University and recorded on the accompanying coversheet. Any significant change to recommended encryption standards by the UK Information Commissioner and/or the CESG, legislation, or University Policy or procedures primarily concerned with information *confidentiality, integrity and accessibility* may trigger an earlier review. These Regulations will be presented to the University Principal's Office for approval.

13. Monitoring

IT Services will monitor and assess the extent to which mobile devices provided by the University are being encrypted. The University may from time to time assess (remotely) if devices connected to its network have been encrypted.

14. Reporting breaches

In the first instance any suspicion of a breach of these Regulations should be reported to the University IT Help Desk, or the University Associate Chief Information Officer (Information Assurance & Governance).

Where a serious breach of the DPA has occurred i.e. where a substantial loss of, or unauthorised access to personal information has occurred (volume or sensitivity) - where the potential harm to individuals has become an overriding consideration, then the University may report the matter to the UK Information Commissioner. If there is a belief that the DPA has been breached where personal and/or sensitive personal data may have become compromised, the University Associate Chief Information Officer (Information Assurance & Governance) should be advised in the first instance.

15. Loss of and/or compromise of ICT facilities

The loss and/or compromise of ICT facilities made available to Authorised Users via IT Services should be reported to the IT Help Desk at the earliest practical opportunity. The

loss of ICT facilities made available via Schools and Services should be reported to the appropriate Head of School or Service, or their nominee. The theft of ICT facilities should be reported to the University's Head of Security or their nominee.

16. Sanctions

Failure of an Authorised User to comply with this Policy may result in access to University ICT facilities being denied (either on a temporary or permanent basis), and/or disciplinary action being taken depending on the severity of the breach under the University's disciplinary procedures (as applicable). Where contractual terms have been broken the University will review its position with that party. This could lead to termination of a contract of employment, studies, research or the provision of goods/services. Where it is believed that a criminal action has occurred, the University will also report this to law enforcement agencies. The University also reserves the right to advise third parties of any infringements of their rights, and to pursue civil damages against any party.

17. Availability

This Policy will be published on the University Website. The Policy can be made available in different formats, please direct any requests to the Associate Chief Information Officer (Information Assurance & Governance).

18. Contacts/further information

Enquiries regarding these Regulations can in the first instance be directed to the University Associate Chief Information Officer (Information Assurance & Governance).