UNIVERSITY OF WOLVERHAMPTON ENCRYPTION POLICY

POLICY ON PROCESSING PERSONAL DATA AND SENSITIVE INFORMATION OFF CAMPUS OR ON AN EXTERNAL NETWORK (‘THE ENCRYPTION POLICY’)

1. PURPOSE AND SCOPE

1.1. This document sets out the University’s policy on processing personal data and sensitive information off campus or on an external network, including the use of portable and mobile equipment.

1.2. Its aim is to ensure that the University complies with data protection legislation and that sensitive information is protected from unauthorised access, dissemination, alteration or deletion. It complements and supports the existing **Data Protection Policy** and **Information Governance Policy**.

1.3. It applies to all University staff students and others who process sensitive information off campus or on external networks on behalf of the University. It covers the use of mobile devices (e.g. laptops, tablets, and smartphones), portable storage media (e.g. memory sticks or CDs), remote computers, or other forms of communication (e.g. email and instant messaging) as well as Cloud based storage provided as a service not provisioned by the University of Wolverhampton.

2. POLICY DEFINITIONS

2.1. **Processing** – means any operation on data, including organisation, adaptation and alteration; retrieval, consultation or use; disclosure, transmission, dissemination and otherwise making available; or alignment, combination, blocking, erasure and destruction. Processing includes the sending of information via email and other mechanisms such as Instant Messaging and Twitter.

2.2. **Sensitive information** – includes, for example, confidential information, information critical to the business continuity of the University, research data subject to contractual non-disclosure agreements and information held in business critical applications. Further examples are given below.

2.3. **Personal data** – the legal and technical definition of ‘personal data’ is complex, however staff should treat information about living, identifiable individuals as ‘personal data’. Specific examples are given in 7 below.

2.4. **External network** – is either provided by a third party (for example an ISP or mobile provider) or is part of the University’s guest network provision (including EduRoam). This covers any use of mobile devices when processing University information.

2.5. **Encryption** – the process of converting information so that it cannot be read by unauthorised people.

3. CONSEQUENCES OF NON-COMPLIANCE

3.1. Failure to comply with this policy may expose the University, its staff or students to risks including fraud, identity theft and distress, or damage the University’s reputation and its relationship with its stakeholders, including research funders. Regulators can impose punitive penalties on the University for breaches of data protection legislation.

3.2. Failure to ensure data is adequately protected and processed in compliance with this policy may result in disciplinary action being considered against the ‘data owner’ by the University of Wolverhampton.

4. BACKGROUND

4.1. The Data Protection Act 1998 sets out how the University may use personal data. Principle seven of the Act states:

4.2. *'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'*

4.3. Compliance with the above Principle involves a judgment as to what measures are appropriate in particular circumstances; this policy provides guidance on how to make this judgment when processing high risk personal data or sensitive information on an external network. Regulators in other jurisdictions also have requirements for keeping data secure.

4.4. The University of Wolverhampton will as a minimum standard apply all UK law relevant to data handling and processing. All University of Wolverhampton data and information will be deemed to be processed or accessed within UK legal jurisdiction. Additional legislation may apply to students, staff or partners operating outside the UK. It is the user's responsibility to ensure they comply with the legal requirements of the country they are operating from, however the UK legal requirements will apply irrespective on local legal requirements and in addition to local legal or regulatory requirements.

5. POLICY STATEMENT

5.1. This policy applies to all users of information owned by the University of Wolverhampton that is defined as Classified Data[1] or that is of a confidential, sensitive, personal or of commercial value.

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

5.3. If Classified Data which is designated as 'Highly Confidential' or 'Confidential[2i] is to be processed off campus or on an external network, then it must be stored and transmitted in an encrypted form of the required standard.

5.4. Any exceptions to this policy statement must be authorised by the Director, Directorate of Academic Support.

5.5. **EXERCISE CAUTION** – Information Governance Policy requirements must be adhered to if any of the following apply:

- Using a personally-owned computer or device (tablet computer, smartphone, etc.)
- Using an appropriately secured Wi-Fi connection whether on or off campus
- working in a public or non-UoW office (e.g. another company or at home)

5.6. **NORMAL BUSINESS** - normal policy for handling personal or sensitive data (as defined by the Data Protection Policy) will apply:

- working on University premises
- Using a University owned computer/device
- computer/device is directly connected to the UoW network via a network cable to a port which is not designated for guest access

[1] See Data Classification Guidance document for definition of Classified Data – University of Wolverhampton (2016)

[2] Information Governance Policy – University of Wolverhampton (2016)

6. KEY PRINCIPLES

6.1. The following key principles underpin the policy statement in paragraph 5 above and this policy generally. All staff must comply with these principles when using mobile devices and portable storage media or otherwise processing personal data, sensitive information or Classified Data on an external network.

- Avoid processing personal data whenever possible.
- If processing personal data is necessary, then consider anonymising the information to obscure the identity of the individuals concerned
- Use the University's central shared drives to store and access Classified Data including personal data and sensitive information; this helps to ensure that only legitimate users have access to it.
- Use the IT-authorised remote access facilities to access Classified Data including personal data and sensitive information on the central servers instead of transporting it on mobile devices and portable media.
- Do not use non IT-authorised third party hosting services, like Dropbox or Google Mail, when processing Classified Data designated as 'Highly Confidential' or 'Confidential' or which includes high risk personal data or sensitive information.
- Only use mobile devices, portable media or email for Classified Data or high risk personal data or sensitive information which use encryption.
- Do not use personal equipment, such as home PCs or personal USB sticks, to process Classified Data including confidential personal data or sensitive personal information.
- Do not send Classified Data including confidential personal data or sensitive personal information by email or using email to store such information. If you must use email to send this sort of information please ensure you encrypt it with a University approved encryption tool.
- Only University of Wolverhampton email accounts may be used for the communication of Classified Data including confidential personal data or sensitive personal information. Under no circumstances will commercial Web based personal email accounts be used for the transmission of any Classified Data including confidential personal data or sensitive personal data.
- Do not process Classified Data or high risk personal data or sensitive information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted Classified Data including high risk personal data or sensitive information to an insecure device.
- Consider the physical security of Classified Data including high risk personal data or sensitive information, for example use locked filing cabinets/cupboards for storage.
- Implement the University's **records management policy** and **retention and disposal policies** so that you do not keep personal data and sensitive information that you do not need. If there are no suitable retention and disposal policies in place for your area, contact your Senior Information Risk Officer (SIRO) to arrange to put some in place.
- Where the master copy of record is held in an electronic form, it should be stored on university servers. In identifying master copies of record, staff should seek advice from their SIRO.

- Electronic keys for encryption, e.g. passwords, must be appropriately managed so that the University can always access the information. This is a critical requirement where employment is terminated and the Line Manager of the member of staff is responsible for securing all encryption keys prior to the staff members' departure.
- Each Faculty, Department and partnership organisation will be responsible for ensuring that encryption keys for encrypted data are retained post-employment to ensure data access is retained for a period of five years post-employment of the member of staff.
- Each Faculty, Department and partnership organisation will ensure that a record of encryption keys is retained for a period of five years post completion of research projects. A copy of the encryption software will be retained to ensure legacy access for research data is maintained during the retention period.
- It should be noted that loss of the decryption key will likely mean that no-one will be able to gain access to the data. Loss of the decryption key could constitute an 'accidental loss or destruction of, or damage to, personal data' and would therefore be a breach of the seventh principle of the Data Protection Act.
- When sending encrypted data outside the UK, have regard for the regulatory regime in the destination country. UK law will be the minimum requirement for compliance, destination legal requirements will be in addition to the UK legal standard.
- Ensure that any third party working with any University-owned information as set out under section 7 below handles it in accordance with the policy statement under section 5. This includes ensuring that, where such data is returned from that third party to the University, it is transmitted in encrypted form.
- Encryption keys, e.g. passwords, must not be communicated via the same channel as the encrypted data. Contact ITS Service Desk (ext. 2000) for approved transmission protocols or procedures.

7. CLASSIFIED DATA - HIGH RISK PERSONAL DATA OR SENSITIVE INFORMATION

7.1. The following are examples of high risk personal data or sensitive information identified by the Information Commissioner Office, loss of data in this category would constitute a reportable data breach (See: Data Classification Guidance[3])

- Any set of data relating to more than 50 living, identifiable individuals, including, but not limited to, students, staff, alumni, research participants.
- Any set of data relating to 10 or more living, identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary.
- Information relating to 10 or more members of staffs' performance, grading, promotion or personal and family lives.
- Information relating to 10 or more alumni/students' programmes of study, grades, progression, or personal and family lives.

[3] : Data Classification Guidance (Appendix 6) for Data Breach Reporting Process.

- Any set of data relating to 5 or more living, identifiable individuals' health, disability, ethnicity, sex life, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence.
- Information relating to identifiable research participants, other than information in the public domain.
- Information that would be likely to disadvantage the University in funding, commercial or policy negotiations.
- Information provided to the University in confidence.
- Finance data held in Agresso.
- Health records of any living, identifiable individual.
- Discussion papers and options relating to proposed changes to high profile University strategies, policies and procedures, such as the University's undergraduate admissions policy, before the changes are announced.
- Security arrangements for high profile or vulnerable visitors, students, events or buildings while the arrangements are still relevant.
- Information that would attract legal professional privilege.

8. ACTION ON LOSS OR THEFT OF DATA

8.1. If a University-owned mobile device (laptop, smart phone, tablet etc., or storage media) is lost or stolen this should, in the first instance, be reported to the User's Line Manager. If a device is lost that holds confidential, sensitive or commercially valuable information belonging to the University of Wolverhampton, the loss must be reported to the IT Service Desk (ext. 2000) within 36 hours of discovery of the loss or 24 hours if the data consists of Highly Confidential business data[4], 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.

8.2. The Data Classification Guidance document (Appendix 6) provides a reporting flowchart for lost/stolen data or devices. Managers should be aware of the time constraints for reporting lost data/devices, failure to report a loss within the time constraints may result in disciplinary proceedings.

9. REQUIRED ENCRYPTION STANDARDS

9.1. The required standard of encryption is AES 256 bit, FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197. Encryption products certified via CESG's CPA or CAPS schemes to at least FOUNDATION grade would also meet the required standard.

9.2. All University managed devices will have hard disk drive encryption enabled to encryption standard AES-256.

10. ENFORCEMENT OF POLICY

10.1. 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, students and partners provided with IT accounts 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.

[4] Data Classification Guidance – Section 3

11. GUIDANCE AND SUPPORT

11.1. Further support is available from:

- OURS Data Protection Officer on records management and data protection
- IT Service Desk (ext.2000) on the technical aspects of security
- University of Wolverhampton Regulations – www############

END OF DOCUMENT

Version	1.1	Author	Stephen Hill
Approved Date	15th June 2016	Approved by	InfoSec Project Board (CMT)
Review Date	September 2017		