Information Management and Policy Services (IMPS) and Digital Technology Services (DTS)

Encryption Policy

1. Purpose and scope

This policy applies to all University staff that handle University data and confidential information and sets out the framework within which the University will manage the security of the information for which it is responsible, maintaining an appropriate balance between accessibility and security. This document sets out the University's policy on processing *high risk* data and *sensitive* information off campus or on an external network, including the use of portable and mobile equipment. Its aim is to ensure that the University complies with data protection laws and other legal obligations and that University data is protected from unauthorised access, dissemination, alteration or deletion.

For the definition of 'high risk and sensitive' information please refer to Section 5. Further definitions can be found in the Glossary, Section 8.

1.1 The University recognises the need for its staff to be able to disseminate, store and transport the information they require in order to carry out their work.

1.2 The University also recognises that the information it manages must be appropriately secured in order to maintain its reputation for trustworthiness, to protect against damage and/or distress being caused to those that entrust us with their data, to protect the institution from the consequences of breaches of confidentiality including possible legal and financial consequences , to avoid failures of integrity or interruption to the availability of that information and to comply with the law and any applicable contractual agreements.

1.3 This policy applies to all information for which the University has a legal, contractual or compliance responsibility, whether that information is stored or processed electronically or by other means.

1.4 This policy applies to the use of mobile devices (e.g., laptops, tablets, and smartphones), portable storage media (e.g., USB memory sticks, portable hard drives, CDs or DVDs), remote computers, or other forms of communication (e.g., websites, email and instant messaging).

1.5 This policy applies to all staff or any other person or organisation having access to University data.

1.6 This policy complements and supports the existing **Data Protection Policy, Information Security Policy, Classification Policy, Records Management Policy, Information Security Incident Response Policy, Regulations for the Use of the University of Reading's IT Facilities and Systems** and **guidance on the handling of payment card data in line with PCIDSS compliance requirements.**

2. Roles & Responsibilities

Heads of Schools, Functions and Departments	To ensure that their staff are made aware of this policy and that breaches of it are dealt with appropriately.
Line Managers	To ensure that their staff are aware of the Policy, the Regulations on the Use of IT Facilities, and any other Information Security Policies relevant to their work. To ensure that staff and other people with access to personal data and sensitive Information undertake the Information Security training prior to being given access to University data and systems. To ensure that the business processes and practices in their areas comply with the Information Security Policies and other obligations concerning confidentiality.
Information Asset Owners, Stewards and Custodians	To ensure that an appropriate security classification is applied to the Information they are responsible for, and that encryption of high-risk data and sensitive information is applied where required. To ensure that the business rules covering access rights to the service are defined and maintained, and that they are compatible with the security classification of the underlying information. To ensure that the information security risks for the service are identified, assessed and addressed prior to implementation, and reviewed at regular intervals thereafter. To ensure that information assets are effectively managed in accordance with the data protection principles and Data Protection Policy. To assist with any Information Security Incident as part of the Information Security Incident Response procedures.
University staff	To assess the need for encryption, based on requirements set out in this policy and apply appropriate security measures as needed. To comply with the Regulations on the Use of Digital facilities, including payment device systems. To complete all required training and follow related policies and guidance.

	To report any breaches or suspected breaches of Information Security in accordance with the Information Security Incident Response Policy. To inform DTS of any potential threats to Information Security, including ecommerce or payment systems.

3. Consequences of Non-Compliance

3.1 Failure to comply with this policy may result in the University revoking your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether the breach takes place at your normal place of work.

4. Requirements and Key Principles

The following key principles underpin this Policy.

4.1 If processing personal data on external networks or devices staff must first consider whether anonymising the information to obscure the identity of the individuals concerned would be possible. Further guidance on anonymisation can be found at Information Commissioner's Office Anonymisation guidance.

4.2 University managed IT services are appropriately secured and backed up so use these wherever available. The University Virtual Private Network (VPN) must be used to access some systems when working off-site. Connect to the VPN regularly when working off-site even when not accessing systems that require VPN; this enables important security updates to run.

4.3 If high-risk or sensitive information is to be processed off campus or on an external network, then it must be stored and transmitted in an encrypted form. This includes the encryption of files sent by email, data in transit held on portable hard drives, and in the case of websites or e-commerce, the use of encrypted transmission protocols such as SSL. There are exceptions where access or transmission of high risk or sensitive information is being conducted using University managed systems such as University managed email and cloud services. Some examples are provided below:

Activity	Do I need to Encrypt?	Notes
Using a personally owned device to process high risk or sensitive information	Yes - Device	Use is also subject to the BYOD Policy
Accessing University issued email accounts of Campus	No	Existing University managed security measures will apply
Accessing University managed systems (e.g., RISIS, Agresso) off site via	No	Existing University managed security measures will apply

University approved access routes		
Sending High Risk or Sensitive Information to or from a non-University issued email account	Yes	Contact IT if you require installation of currently approved encryption software
Creating a website or ecommerce site that will involve the transmission of high risk or sensitive data	Yes	Seek advice from your IT business partner in the first instance
Storing high risk or sensitive information on a portable hard disk or USB	Yes – device or files	Before using portable devices consider if there are alternative ways to store information on site or to share using University managed collaboration tools or areas

4.4 Staff should not use *non*-University managed third party hosting services, like Dropbox or Google mail/storage, when processing high risk or sensitive information. Seek advice from IMPS or IT regarding University approved alternatives (such as One Drive) or to seek authorisation for use by exception, for example, where necessary for reasons of Business Continuity and Major Incident planning and response.

4.5 Staff should not process high risk or sensitive information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high risk or sensitive information to an insecure device. Please refer to University Policies on remote working for additional requirements for working off campus.

4.6 When sending encrypted data outside the UK, staff should have regard for the regulatory regime in the destination country. Be aware when travelling abroad that government agencies may require you to decrypt information on entering or exiting a country. Wherever possible avoid travelling with high risk or sensitive information. Seek advice from IMPS or IT if required.

4.7 Third party hosted data, for example where external suppliers are used, including software as a service, cloud hosted solutions and third-party web-based applications will be subject to due diligence checks, including but not limited to, those assessed by the University Design Authority Group, to ensure they can afford an appropriate level of security for personal data. When requested you may be required to obtain information pertaining to supplier security and encryption measures on request.

Devices

Laptops, smartphones, tablets – University owned

4.8 All University owned laptops, smartphones and tablets shall be encrypted unless in exceptional instances where this is not deemed necessary

4.9 The University's centrally approved encryption solutions will be used, and all encryption keys, passwords, passphrases or other keys must be robustly managed to ensure accessibility of

data when required. Seek advice from DTS if you need to check recommended encryption tools.

Laptops, smartphones, tablets – Personally owned

4.10 All staff using personally owned devices must comply with the requirements of the Bring your own device (BYOD) Policy.

4.11 Staff should wherever possible avoid the storing of high risk or sensitive information on personally owned devices. Where this is unavoidable, staff must encrypt the device using IT approved encryption standards. Staff will be wholly responsible for the safe management of their encryption keys, passwords and any other means of access; IT will be unable to recover lost passwords for personally owned devices and staff should be aware that loss of passwords or encryption keys could render data inaccessible. For this reason, you must ensure that copies of the data are maintained on University systems to protect against risks posed by data becoming inaccessible.

Other portable devices/removable media

4.12 Portable devices such as USB sticks, portable hard drives, and recording devices are at higher risk of loss or theft so additional care must be taken to protect the physical security of these devices.

4.13 Wherever available, device encryption should be used ensuring that encryption keys, passwords and any other means of access are stored securely on University networks.

4.14 Alternatively, encrypt files that will be stored on the device.

4.15 Encryption is a *mandatory* requirement for any portable devices/removable media that will be used to store or transfer high risk or sensitive information.

Email and data sharing tools

4.16 Avoid sending high risk or sensitive information externally by email or using email to store such information. If you must use email to send this sort of information externally, encrypt it prior to sending.

4.17 If you are sending unencrypted high risk or sensitive information to another *internal University email account*, to include any accounts issued by the University, take extra care that you have the correct recipient, indicate in the email subject line that the email contains sensitive or confidential information so that the recipient can exercise caution about where and when they open it. This includes those invited to view documents within cloud-based storage e.g. One Drive. Password protection for internally transmitted documents is advisable and may be mandated by the DPO in instances of recurrent errors involving incorrect recipients.

4.18 Ensure that any third party working with any University data that involves high risk or sensitive information handles it in accordance with this policy.

4.19 Encryption keys, e.g., passwords, must not be communicated within the same channel as the encrypted data, for example, do not send a password within the same email as the encrypted information, or a USB stick together with the password.

4.20 Suspected or confirmed compromises of *personal data* (irrespective of classification or being high risk or sensitive information) must be reported to the IMPS team promptly in line with

the requirements of the University Information Security Incident Response Policy. Lost or stolen University issued IT devices should also be reported to IT immediately.

4.21 Use the University's central and secure shared drives to store and access high risk and sensitive information wherever possible; this helps to ensure that only legitimate users have access to it as well as ensuring it can be readily accessed.

4.22 Use the IT-authorised remote access facilities (such as VPN) to access University data on the central servers instead of transporting it on mobile devices and portable media wherever possible.

5. High Risk data and sensitive information is that falling within any one of the below:

- Any data defined as Highly Restricted under University information classification.
- Credit/Debit card numbers.
- 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 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.
- 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.
- Confidential information critical to the business continuity of the University, and information held in business-critical applications.
- Any information or data that is subject to non-disclosure agreements or any other contractual confidentiality obligations.
- Information provided to the University subject to contractually binding requirements governing the use of Encryption.
- Finance data held in Agresso and any credit/debit card data covered by PCIDSS security requirements. (https://www.reading.ac.uk/finance/ecommerce-and-payment-solutions/pci-dss-compliance)
- 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.

6. Where to go to for advice

Advice on how to encrypt University owned devices and approved encryption tools and standards

IT

its-help@reading.ac.uk 0118 378 6262

Advice on when and how to encrypt files for transmission outside of the University

http://www.reading.ac.uk/internal/imps/DataProtection/DataProtectionAdditionalInformation/ITSsharedsections/imps-d-p-encryption-files.aspx

IMPS Information governance, records management and data protection

imps@reading.ac.uk 0118 378 8981

Ecommerce - Payment security and PCI-DSS

ecommerce@reading.ac.uk

7. Related policies, procedures, guidelines or regulations

Key related policies and rules:

- Information Security Policy
- Data Protection Policy.
- Classification Policy
- Regulations for the Use of the University of Reading's IT Facilities and Systems
- Related Information Security Policies listed at: http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx
- Equal Opportunities Policy
- Information Security Incident Response Policy

Policies superseded by this policy

Encryption Policy v1.0,1.2,2.0,2.1,3.0

Overall responsibility for this Policy lies with the University Senior Information Risk Owner (SIRO)

8. Review

This Policy shall be reviewed at regular intervals and documented within the version history. Reviews will take place as a minimum at the documented frequency and in the event of any of the below:

- Significant change in University operations
- Significant change in legislation, regulatory requirements, industry guidance or similar
- In the event of a compromise of data protection or security where the content or compliance with this policy is identified as an aggravating or mitigating factor
- Any other identified requirement necessitating substantive changes ahead of scheduled review

9. GLOSSARY

Data Protection Laws	means the General Data Protection Regulation 2016/679, the Data Protection Act 2018 and any other applicable data protection laws.
DPO	means the Data Protection Officer.
SIRO	means the Senior Information Risk Officer (the University Secretary).
IMPS	means the Information Management and Policy Services department.
IT	means the IT department.
Information Asset Owner	means the designated owner of risks associated with specified information assets (IAs), responsible for actioning quality and security controls.
Data Steward	means the designated owner of risks associated with specified Information Asset systems, responsible for data quality within the IA system, providing assurance on quality and security to Information Asset Owners, conducting granular risk assessments and overseeing the implementation of quality and security controls.
Data Custodians	Means the person (s) responsible for the technical environment, for example IT Support.
Staff	**Includes:** - Employees (including temporary or short-term workers) of the University or a subsidiary company of the University. - Volunteers, interns and those undertaking placements or work experience. - Contractors engaged by the University. - Students working for and/or on behalf of the University, including Postgraduate Research students.

	- Those with University accounts by virtue of a visiting or courtesy title conferred by the University. - Any other individual who is working on behalf of the University if they are processing University data or information.
High Risk Data	means that defined in Section 5 of this policy.
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 Social Media.
Sensitive information	means that defined in Section 5 of this policy.
Personal data	means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
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 data.
Encryption	the process of encoding data, information or messages in a way that unauthorised persons cannot read it but those that authorised (hold the key or password) can.

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
1.0 No longer in use							
1.2 No longer in use							
2.0		IMPS	DEC 19	University Policy Group	DEC 19	DEC 19	DEC 21
2.1	Section reference corrected	IMPS					DEC 21
3.0		CISG	FEB 22	University Policy Group	APR 22	APR 22	APR 24
3.1	8. Review period added	IMPS	AUG 23	IMPS			APR 24
3.2	Next review period amended	CISG	JUL 25	CUUP	JULY 25	JUL 25	APR 26