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

Activity	Do I need to Encrypt?	Notes
Using a personally owned device to store high risk or sensitive information		

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 held centrally to ensure accessibility of data when required.

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

- 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 payment card data covered by PCIDSS security requirements.
- 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.
- information that is marked as confidential.

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

- 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 v1.2

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

8. 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	PPOrall re □1 y

- Employees (including temporary or short term workers) of the University or a

Document control

SECTION	KEEPER	REVIEWED