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

Information Security Policy

1. Purpose and scope

This policy applies to all University staff that handle University data 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.

1.1 The University recognises the need for its staff to have access to 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 the institution from the consequences of breaches of confidentiality, failures of integrity or interruption to the availability of that information and to comply with the law and to comply with contractual agreements.

1.3 The University must demonstrate that it complies with the obligations contained within:

- The General Data Protection Regulation 2016/679 and UK GDPR
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- The Counter Terrorism and Security Act 2015 (in particular the 'prevent' duty')
- The Payment Card Industry Data Security Standard (PCI DSS)

1.4 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 (the Information).

1.5 This policy is concerned with the confidentiality, integrity and availability of the Information (the Information Security).

1.6 This policy applies to the equipment, systems, credentials, etc. that are used to access the Information, safeguard Information Security, or could have some bearing on Information Security (the Information Systems).

1.7 This policy applies to all staff or any other person or organisation having access to the Information or Information Systems.

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

For the definition of 'high risk and sensitive' information please refer to Section 5.

Further definitions can be found in the Glossary in Section 8.

2. Roles & Responsibilities

University's Risk Management Group (RMG)	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. Review and approve the annual corporate risk register, and receive progress and outcome reports Receive the reports on High-Risk Information Security Incidents. Take advice from the CISG on Information Security matters.
Cyber and Information Security Group (CISG)	Implementation, monitoring, and review of this policy. Approve Information Security Policies in conjunction with the Policy Group as required Refer Information Security issues to the RMG as required.

	Receive reports on Information Security incidences and issues from IMPS and DTS.
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 DTS 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 information 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.
University staff	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 can lead to

- damage and distress being caused to those who entrust us to look after their personal data, risk of fraud or misuse of compromised personal data, a loss of trust and a breakdown in relationships with the University.
- damage caused by unavailability, inaccessibility or corruption of University information assets.
- damage the University's reputation and its relationship with its stakeholders (including research funders and prospective students and collaborators).
- Significant legal and financial consequences. Monetary penalties of the Information Commissioners Office can reach up to twenty million euros or 4% of turnover. Individual civil action for breaches of data protection can also be taken by individuals.

Failure to comply with this policy may result in us 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 or not the breach takes place at your normal place of work.

4. Key Principles and Requirements

The following key principles underpin this policy statement.

- The University will maintain an appropriate balance between convenient access to information and security of that information which will be a critical element of the University's information systems.
- The level of Information Security to be applied in individual circumstances shall be driven primarily by the Classification of the Information concerned and consideration of the risks involved.

- University information will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- This shall be achieved by an appropriate mix of policies, standards, guidelines, technical measures, training, support, audit and review.
- This policy is the primary policy under which all other technical and security related polices reside. This Policy, together with subsidiary policies and implementation documents, available from: http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx
- Training in the fundamentals of Information Security shall be mandatory for all staff and other people with access to University Information. Regular refresher training will be a requirement and made available to staff to complete in order to ensure training and guidance remains up to date and takes into account emerging and evolving threats and changes to best practice advice.
- Information Security risks shall be assessed annually and be documented as part of the Corporate University Risk Register. This shall include measures such as, but not limited to, internal and external review, audit and penetration testing.
- Significant residual risks to University information will be referred to the SIRO for assessment and approval.

The following are requirements that underpin this policy statement that apply to all staff.

- Seek advice from DTS or IMPS if you are unsure about Information Security;
- Complete all Information Security training as required or requested;
- Ensure all devices are protected by strong password (in line with University guidelines) as a minimum. If using personally owned devices, ensure that use meets the requirements of the University Bring Your Own Device Policy;
- If sending or transporting University Information externally ensure that this meets the requirements of the University Encryption Policy;
- Do not share or re-use passwords;
- Do not permit access to University information to those that are not authorised to view it;
- Do not use non-University issued email accounts for University business;
- Do not leave your devices unlocked when unattended;
- Ensure locations where High Risk or Sensitive information is held or stored are locked when unattended.

- Do not leave High Risk or Sensitive information in plain view; keep a clear desk when away from your workstation
- Report any suspected or confirmed compromises of University information to IMPS immediately;
- Report any suspected or confirmed suspicious activity on your accounts, including malware or viruses to DTS immediately;
- Be aware that the University may need to conduct due diligence assessments of security including those relating to software acquisition, external suppliers, integrations, data hosting, contractual requirements, and back-up and recovery prior to approval, implementation or use;
- Be aware that the University reserves the right to mandate encryption of portable devices, multi factor authentication and remote wipe functionality if for the purposes of supporting appropriate organisational and technical measures regarding Information Security.

5. High Risk data and sensitive information is:

- 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 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 further advice

IMPS Information governance, records management and data protection

imps@reading.ac.uk 0118 378 8981

https://www.reading.ac.uk/imps/data-protection/data-security

DTS Information Technology, encryption methods, device management

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

https://www.reading.ac.uk/digital-technology-services/cyber-security

Ecommerce - Payment security and PCI-DSS

ecommerce@reading.ac.uk

7. Related policies, procedures, guidelines, or regulations

Key related policies and rules:

- Encryption Policy.
- Data Protection 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
- Bring your Own Device (BYOD) Policy
- Information Security Incident Response Policy

Policies superseded by this policy

Information Security Policy v1.1.2

Information Security Policy v1.0

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	means the Data Protection Officer.
SIRO	means the Senior Information Risk Officer (the University Secretary).
IMPS	means the Information Management and Policy Services department.
DTS	means the Digital Technology Services (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 DTS 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
1.1.2 - No longer in use							
1.0		IMPS	DEC 19	University Policy Group	DEC 19	DEC 19	DEC 21
2.0		CISG	Apr 22	University Policy Group	APR 22	APR 22	APR 24