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

University of Reading

# Information Classification 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 classification of the information for which it is responsible and the related handling requirements for information, based on those classifications.

1.1 The University has a Data Protection Policy and an Information Security Policy, which jointly aim, amongst other things, to ensure that the availability, security and integrity of its information are appropriately safeguarded, whilst not imposing any undue burdens on staff.

1.2 A key element of striking this balance is the recognition that some types of information require more protection, and therefore more careful handling, than others. By targeting more restrictive requirements at the more sensitive types of information, an appropriate balance of security versus convenient access and use can be reached across a broad range of types of information.

1.3 In order to be consistent in the application of this principle, it is important to have an agreed scale of information sensitivity, and a clear set of processing requirements that apply to each point on that scale.

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

- The UK General Data Protection Regulation
- 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.

1.5 This policy defines a set of information security classifications, together with criteria for allocating the appropriate classification to any particular category of information, and descriptions of the general safeguards to be applied in the handling of information in each of the defined categories.

1.6 This policy does not detail the specific techniques to be used to achieve the general safeguards. For example, the policy might require strong encryption to be considered when storing or highly restricted information but will not specify the encryption algorithms to be used. Reference should be made to internal guidance from DTS and IMPS for this level of information.

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 applies both to Information Sets and in some cases to individual records within Information Sets, where the appropriate classification for the record differs from the Information Set as a whole

1.9 Some information that the University processes will originate outside the University and may bear a security classification from the originating organisations. Such information still falls within the scope of this policy.

1.10 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 IT (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

| | |
|---|---|
| **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 Management Policies relevant to their work.<br>To ensure that staff have completed all mandatory courses in Data Protection and Information Security.<br>To ensure that due regard is given to the handling requirements of classified information. |
| **Information Asset Owners, Stewards and Custodians** | To ensure that an appropriate classification is applied to the Information they are responsible for.<br>To ensure that the necessary details of the information they are responsible for are passed on to the Data Protection Officer if requested. |

| | |
|---|---|
| | To ensure that the business rules covering access rights to the service are defined and maintained, and that they are compatible with the information classification of the underlying information.<br>To ensure that any contractual requirements regarding the handling of classified information are adhered to.<br>To ensure that information assets are effectively managed in accordance with the information classifications, data protection principles and Data Protection Policy. |
| **University staff** | To comply with the requirements for handling University Information in line with Information classifications.<br>To complete all required training and follow related policies and guidance.<br>To report any breaches or suspected breaches of Information Security in accordance with the Information Security Incident Response Policy.<br>To inform DTS of any potential threats to Information Security. |

## 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.

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. Requirements and Key Principles

The following key principles underpin this policy statement.

- The University is committed to achieving an appropriate balance of security and convenience of access and use across a broad range of types of information by the definition and application of a system of Information Security Classification.
- All information falling within the scope of this Policy shall be classified as:
    - Unrestricted;
    - Restricted; or
    - Highly Restricted.
- **Unrestricted** Information is information that can be made freely available to the public. It shall **not** be applied to any information that:
    - Would be defined as Personal Information under the General Data Protection Regulation 2016, except where public disclosure is in compliance with the University's Data Protection Policy ; or
    - Falls under one of the exemptions listed in the Freedom of Information Act (FOIA) 2000; or
    - Is not permitted to be released to the public by virtue of a contractual or other legal obligation on the University; or
    - Carries a security classification applied to the information by an external organisation, and which the University may reasonably be expected to abide by.
- **Restricted** Information is information that shall not be made public and shall only be handled by members of well-defined groups of individuals that have a reasonably foreseeable need. It might, for example, include personal information, commercially sensitive information or information originating elsewhere that has been made available to the University on a restricted or confidential basis.
- **Highly Restricted** Information is information that shall be restricted to a small number of named individuals, each with a clearly defined need. It might, for example, include sensitive personal information, such as details of health status, or information with the potential to cause harm to individuals or to the University if compromised lost or disclosed, such as financial data or payment details, or information with the potential to prejudice the investigation or facilitate the commission of crime, such as reports held by our Security team. It will also include information subject to stricter controls imposed by those we work with and for, for example data pertaining to highly sensitive contracts, or those classified as Secret or Top Secret under the Government Security Classifications (GSC) scheme.
- Non-personal information should be presumed to be Unrestricted unless there are good reasons for access to be Restricted or Highly Restricted. These reasons shall be proposed by the Information Custodian after consultation with Information Management and Policy Services who can assess if any corresponding Freedom of Information Act 2000 exemption(s)

would apply, such as those that provide protections for commercially sensitive information, or information given in confidence.

- Personal information should be presumed to be a minimum of Restricted and only made available to those individuals with a valid reason for access. Access may be relaxed or broadened where there is a demonstrable need for such arrangements and suitable safeguards are in place to ensure compliance with Data Protection Laws and the University's Data Protection Policy. For advice on what qualifies as personal information consult IMPS team.
- The security classification shall be recorded.
- Restricted and Highly Restricted Information should, wherever possible, be clearly labelled as such so that anyone accessing the information or a subset of it is aware of the classification of the information. This should be done for all possible levels, channels and access points, such as document, page, computer system, information set, record, print out etc.
- Where information already carries one or more security classifications from the originating and/or other organisations, and these are binding on the University, these shall be preserved, and a University of Reading classification applied in addition. This classification shall offer at least the same level of protection as the existing binding classification(s).
- Where a record set contains a mixture of records of different classifications, the individual records shall bear the appropriate label, and the record set shall carry a label indicating the highest classification of the records contained. Access to the overall record set shall be managed in accordance with the overall classification, but access to the more restricted records shall conform to the access controls appropriate to those records.
- Business processes and information systems shall be set up to safeguard the security of the different classifications of information during processing as detailed in the following table.

**Additional descriptor/handling labels**

- In addition to classifications of Restricted and Highly Restricted, descriptor labels must be used to indicate the nature of the data and/or any specific restricted audience for the information.
- More than one descriptor can be used

- The below additional category labels can be applied:

| | |
|---|---|
| **PERSONAL** | Where the nature of the data includes the personal data of individuals and security compromise could have damaging consequences for individuals. |
| **COMMERCIAL** | Where the nature of the information is commercially sensitive and security compromise could have damaging consequences for the organisation or third parties commercial, reputational and market interests. |
| **INTERNAL ONLY** | For organisational internal eyes only and not to be shared with external third parties without prior authorisation. |
| **XXXX EYES ONLY** | For use where circulation is strictly limited to a specific group, for example, senior management (XXXX – insert relevant group) |

| Data Classification | Example Type | Example Impact |
|---|---|---|
| **Unrestricted Information** | • Prospectus, course, programme information<br>• General information regarding the University departments, projects, and contacts intended for public audience<br>• Advertising of events, news and activities<br>• Information made available under the Freedom of Information Act (FOIA) publication Schemes<br>• Publicly accessible staff directory<br>• University Policies and procedures<br>• publicly available or accessible research data/outcomes/papers | • No detrimental impact on individuals or University business or operations<br>• Positive Impact on public relations<br>• Positive impact on accessibility and information sources provisions<br>• Positive impact in terms of transparency and open access |
| **Restricted Information** | • Personal data as defined under the General Data Protection Regulation 2016 being any data that can identify an individual with the exception of special category sensitive personal data<br>• Awards, qualifications, attainments of students and staff<br>• Unique personal identifiers including staff and student usernames and ID numbers<br>• Contractual and legal documents | • Breach of confidence and trust in respect of individuals<br>• Breach of applicable Data Protection Laws<br>• Possibility of moderate damage and distress being caused to individuals<br>• Possible grounds for threat of legal action and compensation demands in respect of individuals<br>• Potential for enforcement action from Data Protection Authority extending to significant fines |

| | | |
|---|---|---|
| | • Research data *not* contractually subject to specific handling requirements or external security sensitive classifications (e.g. GSC )<br>• Research data that does not include special category sensitive personal data<br>• Unpublished committee minutes and associated papers<br>• Commercially sensitive data including that relating to planning and University strategy and intellectual property intended for commercial use<br>• Financial data pertaining to accounts held, balances, budgets, salaries, and investments unless subject to publication under FOIA | • Significant detrimental risk to commercial interests of the University or a third party<br>• Potential for increases in spam or malicious use of data |
| **Highly Restricted Information** | • Special category sensitive personal data as defined under the General Data Protection Regulation 2016, being: data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning mental or physical health or data concerning a natural person's sex life or sexual orientation<br>• High Risk data as defined within Section 5 and the University Data Protection and Encryption Policies | • Breach of confidence and trust in respect of individuals<br>• Breach of applicable Data Protection Laws<br>• Significant likelihood of significant damage and distress being caused to individuals<br>• Significant grounds for threat of legal action and compensation demands in respect of individuals<br>• Potential for enforcement action from Data Protection Authority extending to significant fines<br>• Substantial detriment to University business and ability to generate income<br>• Loss of contracts or breaches of contractual terms, financial liabilities |

| | | |
|---|---|---|
| | • Research data contractually subject to specific handling requirements or external security sensitive classifications (e.g. GSC )<br>• Financial data pertaining to account numbers, security codes, or any data that could be used maliciously for the purposes of committing fraud. | • Substantial reputational damage<br>• Detrimental impact on internal staff or student relations |

| Processing | Unrestricted Information | Restricted Information | Highly Restricted Information |
|---|---|---|---|
| **Back Up** | To be considered on case-by-case basis dependant on impact of loss | Subject to having a robust back up process in place. Must not be stored in a manner that risks unavailability, inaccessibility, corruption or loss of data | Subject to having a robust back up in place. Must not be stored in a manner that risks unavailability, inaccessibility, corruption or loss of data |
| **Labelling** | Not required | Required | Required. When transmitted physically, the Highly Restricted labelling shall be concealed by enclosure in a container with no marking applied |
| **Access** | No restrictions | Computing devices used to access the information shall require authentication on each occasion the information is accessed and shall have anti-malware and other security measures as required by IT services. Mobile computing devices shall require device password, code or biometric (fingerprint) access and where possible remote wipe. Fixed computing devices shall be located in physically secure locations. No access shall take place in locations where unauthorised third parties may be likely to see the information | Computing devices used to access the information shall have an appropriate level of security as directed by IT services and shall not be shared with individuals not authorised to see the information. Local storage and caching of the information shall be minimised and protected as far as is practicable. Own devices shall not be used to access the information without encryption. No access shall take place in locations where unauthorised individuals may be able to view or intercept the information. Access via unsecured public Wi-Fi is not permitted |

| | | | |
|---|---|---|---|
| **Storage** | No restrictions | Shall be stored in secure locations / systems within the University, or external facilities that have been approved by IMPS or IT Services. May be stored on password, code or biometric protected portable media for transmission, but not retained thereafter | Shall be stored in secure locations / systems within the University with a minimum of 2 secure barriers, for example a locked cabinet in a locked office. May be stored on encrypted portable media for transmission. Electronic storage within non-University approved systems, databases or software not permitted |
| **Reproduction** | No restrictions | Copies may be made on secure copiers, but must be labelled and handled appropriately and restricted in number to the minimum necessary | Copies to be made only by the originator and to be strictly accounted for |
| **Distribution** | No restrictions | Steps shall be taken to ensure that the information is only available to the authorised recipient groups | May only be distributed to the authorised recipients, for their eyes only. All copies to be recorded and accounted for at all stages in the lifecycle up to and including disposal |
| **Transmission** | No restrictions | May only be transmitted to confirmed or named recipients and following checks of intended recipients. Electronic transfers outside the University subject to requirements in the University Encryption Policy | Maybe transmitted physically by personal courier or secure delivery. Electronic transfers outside the University subject to requirements in the University Encryption Policy |
| **Disposal** | No restrictions | Paper and other non-electronic media to be securely disposed of via confidential shredding. Electronic media to be deleted and/or securely overwritten | Paper and other non-electronic media to be securely disposed of via confidential shredding. Electronic media to be deleted and securely overwritten. Portable electronic media shall be rendered permanently unusable or returned to the University for long term storage. |

**5. High Risk data and sensitive information is:**

- Any data defined as Highly Restricted under University information classification.
- 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.
- 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 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 further advice

**IMPS** Information governance, records management and data protection

imps@reading.ac.uk 0118 378 8981

## 7. Related policies, procedures, guidelines or regulations

Key related policies and rules:

- Information Security Policy
- Records Management Policy
- 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: https://www.reading.ac.uk/imps/information-compliance-policies
- Equal Opportunities Policy
- Information Security Incident Response Policy

## 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

Substantive changes shall be reviewed and approved by the Approving Authority as detailed within Document Control.

Non-substantive, minor, or administrative changes may be made by the Policy Owner, or representative of the Policy Owner, as detailed within Document Control.

**Policies superseded by this policy**

None

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

## 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 Chief Operating Officer). |
| **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:**<br>- Employees (including temporary or short-term workers) of the University or a subsidiary company of the University.<br>- Volunteers, interns and those undertaking placements or work experience.<br>- Contractors engaged by the University.<br>- Students working for and/or on behalf of the University, including Postgraduate Research students.<br>- Those with University accounts by virtue of a visiting or courtesy title conferred by the University.<br>- 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** | | IMPS | NOV 19 | University Policy Group | DEC 19 | DEC 19 | DEC 21 |
| **1.1** | (UK GDPR added) | IMPS | JAN 21 | | | JAN 21 | JAN 23 |
| **1.2** | Review Period Section added<br><br>Classification types expanded | IMPS | OCT 24 | | | | OCT 26 |
| **1.3** | Updated links and roles only | IMPS | Nov 26 | | Nov 26 | Nov 26 | Nov 28 |