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 General Data Protection Regulation 2016/679 and the 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

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

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;

	• Research data *not* contractually subject to

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

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

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:

-