Information Classification Policy

1. Information is the lifeblood of the University, and so its loss or corruption could be catastrophic – both for our operation and reputation. However, not all information needs to be protected and secured in the same way.

2. Therefore an Information Classification Scheme and policy is being introduced in order to improve the handling and enable the better protection of information from accidental or deliberate compromise. It will also help meet legal, ethical and statutory requirements and to promote good practice in information security.

3. The classification scheme covers all information and data held by the University in any format, both electronic and hardcopy. It applies to all users of University information and data; staff, student and external.

4. This classification policy needs to be read in conjunction with the Information Handling Guidelines which give advice and details on how each type of information should be stored, transferred and protected.

5. The classification scheme consists of 4 categories: public, internal, sensitive, and confidential.

Classification	Description	Examples
Public	Information which is designed to be openly available and either provided to those outside the University or may be seen by anyone whether associated with the University or not. **No risk if disclosed.**	Open webpages, prospectus and course information, press releases, leaflets, FOI information
Internal	Non-sensitive or non-confidential information where dissemination is normally only to members of the University, subgroups, partners or suppliers. **Little or no risk if disclosed.**	Most operational University information e.g. committee papers teaching materials, timetables, intranet, policies, guidelines and procedures fall under this category. Unless an item is designed to be public, or needs to be sensitive or confidential, this is the **default classification** for information.
Sensitive	Sensitive information which may be personal, commercially sensitive or legally privileged. Would normally only be available to groups of people who specifically require access as part of their role. Some information designed to be 'public' or 'internal' may start off as sensitive while being developed. **Moderate risk if disclosed**	Budget reports. Some committee and planning papers or parts thereof. Business plans Discussion papers on future strategic plans.
Confidential	Highly sensitive information which would have a significant risk and/or	Staff and student protected personal details (under DPA)

	damaging effect if disclosed or made available. Should only be available to restricted groups of relevant users. **Significant risk if disclosed.**	Sensitive HR information, e.g. information relating to formal procedures. Sensitive financial information. Sensitive planning information prior to wider release.

6. Information should not unnecessarily be put in a higher category than is required. For advice on the correct category see the Appendix or discuss with your line manager or tutor.

7. Some information may change classification during its life, as impact of disclosure or loss reduces.

8. There is no general requirement to actively mark documents with their classification, although it is recommended for confidential to ensure it is appropriately protected. If referral is made to the classification of any information it should only be under the four terms used here.

9. The University has developed policies for how each category of information should be retained, handled and stored. These can be found in the Information Retention Policy and the Information Handling Guidelines.

10. It is permitted to access all types of information from any device using University supplied remote access systems (e.g. RDS), as long as information is not downloaded or stored on the device itself.

11. Before sharing or storing any information, consideration must be given to its probable classification – see Appendix – and therefore whether this is permitted. Anyone using University information has personal responsibility for conforming to this policy.

12. Infringement of these regulations may constitute a disciplinary offence under the applicable process for members of staff or students.

Document control

Version	Author(s)	Owner	Date Approved	Approved by	Review date
1	IE and working group	IT	7 May 2016	ITSPG	May 2017

Appendix – Determining Information Classification

The first table below gives examples of the impact of the disclosure, corruption or loss of availability of each of the information classification categories. The second table gives some questions which could be considered when assessing the classification of information.

	Public	Internal	Sensitive	Confidential
Monetary loss	None	Measurable but not material loss	Loss exceeds contingency budget	Loss affects operation and threatens existence
Staff hours needed to recreate data if corrupted or lost	0 to 10	10 to 100	100 to 1000	Over 1000
Public Relations impact	None	Several negative press mentions	Several weeks of persistent negative media attention	Public relations crisis
Operational Impact	Too small to measure	Minor disruption, recovered on the same day	Significant operational disruption of multiple hours, requiring several days to return to schedule	Multiday disruption materially impacts business plans
Regulatory Impact	None	Requires internal investigation, but no reporting	Reported to regulatory agency, but no investigation	Extended investigation

The questions listed below are provided to assist information owners in properly classifying their information. The importance of each of these items should be rated using a High (H), Medium (M) or Low (L) rating scale. As a general rule of thumb, the more "High" ratings the information receives, the more restrictive the information classification should be.

Classification Question	Rating
How important is it to the University that this information be known only by authorized people?	
How important is it to the University that this data be accurate?	
How important is it to the University that this information be available to authorized people only?	
How important to privacy law compliance is this information?	
How important to regulatory compliance is this information?	
How serious would the impact be if this information reached an unintended audience?	
How likely is it that this information could be used by someone to target employees, students, partners, facilities or operations?	
How valuable would this information be to someone intent on causing harm to the University?	
How likely is it that this information could be used in conjunction with public information to cause harm to the University or its employees, students, or partners?	