University of Bolton

Teaching Intensive, Research Informed

Information Classification Guidance

1. Introduction

1.1 The University processes large amounts of personal information and has an obligation to ensure that it is kept secure and appropriately protected against unauthorised disclosure, access, alteration including loss, theft or destruction. Management of this information is also necessary to ensure compliance with data protection laws and the Freedom of Information Act and Environmental Information Regulations.

1.2 Different types of information require different security measures. Classification is therefore key to ensuring appropriate, consistent and effective data security and management. Each classification listed below determines how information should be handled throughout its lifecycle.

1.3 This guidance applies to all formats of information held by the University, including information and documents relating to University recruitment and admissions, learning, teaching, research and administration records. It is designed to assist staff on how to classify information assets properly and then use them accordingly.

1.4 The examples below are a guide and not an exhaustive list, as the circumstances of each case must be considered in order to assess the harm that may occur to those individuals concerned or impact to the University.

Data Classification	**HIGHLY CONFIDENTIAL**
Description	**Potential to cause significant harm to individuals or the University's interests.** Risk and Impact level: **HIGH** Examples: a) data which includes sensitive/special category information about living individuals and likely to identify those persons consisting of: • *physical/mental health records* • *racial/ethnic origin* • *political opinion* • *religious beliefs* • *trade union membership* • *genetics* • *biometrics (where used for identification purposes)* • *sex life and sexual orientation* • *criminal records, convictions and offences* b) information that links one or more identifiable living individuals with information about them which, if released would put them at significant risk of harm or distress: • *financial information eg salary, national insurance number, bank account details, tax, benefit or pensions records, debt information* • *credit or debit card details* • *passport number* • *individual staff or student records ie. HR system data, SITS system data* • *material related to safeguarding and personal protection matters* • *disciplinary proceedings* • *interview transcripts, research databases or other research records involving individually identifiable sensitive personal data* • *restricted information concerning a large number of people (>500) which may or may not be in the public domain eg. name, address, telephone number*

	c) Data in connection with University business activities and has the potential to impact on the commercial and/or financial interests of the University and its reputation: • *information which is subject to contractual constraints* • *intellectual property* • *Information which may be regarded as highly commercially sensitive* • *legal advice and other information relating to legal action against or by the University* • *information which relates to University security matters* • *reserved committee papers* • *passwords to University IT systems*
Security requirements	This highly confidential information needs considerable safe keeping measures, firmly controlled and limited access and protection. Accessible only by a specified group and/or relevant University staff for a defined purpose.
Any other information where the unauthorised access, disclosure, destruction, loss or theft could cause significant harm and distress to the individual(s) concerned or impact to the University.	

Data Classification	**CONFIDENTIAL**
Description	**Potential to cause harm to individuals or the University's interests.** Risk and Impact level: **MODERATE** Examples: a) Data which links and/or includes personal information about living individuals and it is possible to identify those persons from that data, which may or may not be in the public domain: • *home address/work address* • *home or private mobile telephone numbers* • *date of birth* • *schools attended* • *names of family members or relationships* *b) Records relating to staff and students* • *salary information* • *student assignment marking papers* • *staff/student ID numbers/usernames* • *attendance records* • *examiners comments on student assessments* • *staff/student references (unless contains highly confidential information)* • *course assessments* • *internal correspondence* • *information provided in confidence or under legal privilege* • *student transcripts/exam scripts* • *teaching material including MOODLE content* • *research records and information prior to publication* c) Data in connection with University business activities and has the potential to impact on the commercial and/or financial interests of the University and its reputation: • *tender proposals before a contract agreement has been completed* • *examination question paper released prior to examination* • *financial information* • *policy and planning documents prior to publication* • *key organisational or personnel changes prior to any consultation process* • *reserved committee business/committee papers* • *draft reports, papers and minutes* d) Information that assists in the protection of the University's property: • *access codes to University buildings*

Security requirements	Accessible only by a specified group and/or relevant University staff for a defined purpose.
Any other information where the unauthorised access, disclosure, destruction, loss or theft could cause harm and distress to the individual(s) concerned or impact to the University.	

Data Classification	**NOT CLASSIFIED**
Description	**Information that is not classified as confidential.** Risk and Impact level: **LOW or ZERO** a) Information that is intended to be provided to the public, staff, applicants and students. Examples: • *course information / course prospectus* • *annual reports and financial statements.* • *staff directory (names, job titles and contact details)* • *personal data which has been anonymised* • *committee records* • *information published under Freedom of Information publication scheme* • *information that is publicly available eg. HESA, Office for Students* • *information that is available on the University website*
	Accessible to all members of the public.
Any other information where the unauthorised access, disclosure, destruction, loss or theft is unlikely to cause harm and distress to the individual(s) concerned or impact to the University.	