INFORMATION CLASSIFICATION SCHEME

Organisation	Leeds Beckett University
Author(s)	Head of Information Governance
Developed in consultation with	University Secretary Records and Information Governance Manager
Owner	University Secretariat Office
Target audience	Staff
Sensitivity	Public
Approved by	Information Compliance Team Meeting
Endorsed by	Information Management Operations Group
Effective date	16-07-2020
Review Date	+2 years from last date of approval [08-2022]
Status	Published
External references	
Links to other internal policies / procedures	Information Governance Framework
Version reference	1.00
Version history and summary of changes	No previous versions.

Table of Contents

Introduction

1. Information in all its forms is crucial to the effective functioning and good governance of Leeds Beckett University ('the University') as stated in the University's Records Management Policy which supports the University's Information Governance Framework. The University uses large volumes and diversity of information to support its activities and to achieve its strategic aims. We are committed to efficient and effective information security management that ensures all the information and information capture systems on which the University depends are adequately protected.

Legal and regulatory Framework

2. The University has a statutory and legal duty to ensure that the handling/processing of information complies with the laws and the regulations to which it is accountable. The UKs Data Protection Act 2018 ('DPA 2018') and General Data Protection Regulation 2016 ('GDPR') requires that personal and special category information that the University manages shall be appropriately secured to protect against consequences of breaches of confidentiality, failures of integrity, interruption to availability and failure to comply with legal requirements which is set out in the University's Data Protection Policy.

3. The Information Commissioners Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness and good practice by public bodies and data privacy for individuals. The ICO promotes adherence to a number of acts including DPA 2018, GDPR and Freedom of Information Act 2000 (FOIA). The ICO can issue enforcement notices or monetary penalties of up to 20 million euros (approximately 17 million pounds) or 4% of total worldwide turnover, whichever is higher if it were determined that the University did not take reasonable steps to manage and secure personal information or acted in such a way as to knowingly put information security at risk or caused harm or distress to individuals or groups.

4. All information held in recorded format by the University is subject to the provisions of the FOIA, irrespective of the classification in use. While a request for information under FOIA requires a response from the University, this does not mean that information must be automatically be released where a request has been made. There are circumstances where the University can lawfully withhold the information where it considers that harm could result from the release of the information.

Information Security Risk Management

5. The University's Risk Register Guidance identifies Information Security as an area where the University has a low appetite for risk.

6. There are also significant risks associated with the inappropriate handling/processing of information that carry a high degree of sensitivity. This procedure seeks to improve the management of information whereby the likelihood of information risk is reduced along with any negative harm impact should they occur such as:
   - Harm or distress to individuals or groups;
   - Disruption to the University business activities and/or substantial financial loss;
   - Damage to the University's reputation and standing;
   - Legal action against the University or investigations by regulatory bodies.

7. The protection of information through the application of a business and information classification schemes is one of the most effective regimes available for the protection of personal/special category and business sensitive information. In order to protect information consistently, it is necessary to define a University-wide scheme for classifying (describing) information and how it should be handled according to its requirements for confidentiality, integrity (data quality) and availability.

Purpose and Scope

8. It sets out guidance on the classification of information and information assets and the different levels of security required based on its level of sensitivity, and value to the University. It encompasses all information held by the University, in any format (electronic and hard copy).

9. It ensures that information is clearly identified to alert people to its inherent level of sensitivity and/or confidentiality, against a predefined scale which is designed to help ensure that materials are only made available to those persons with a legitimate right of access.

10. The objectives of this scheme are to:
    - Provide a classification system that is capable of being applied to all information or data created or received by the University, through which an appropriate classification can be assigned; and
    - Define how people should respond to classifications in all aspects of information handling/processing such as creation and alteration, collection, accessing, transmission/dissemination, storing and disposal of information to prevent unauthorised disclosure, alteration or destruction, dissemination or loss.

Responsibilities and/or duties

11. The University's Information Governance Framework sets out roles and responsibilities for Information Governance and Records Management responsibilities. This procedure sets out responsibilities for the classification of information managed within the University. Failure to comply with this scheme could result in a Data Protection Breach and action could be taken as laid out in the section titled Breaches and Sanctions.

Senior Information Risk Owners and Information Asset Owners

12. Senior Information Risk Owners (SIROs) are the senior management with overall responsibility for the use of information as a strategic asset in their School or Service area. Information Asset Owners (IAOs) are responsible for the management of information and Information Assets held in their areas or when their staff capture, and handle/process information held on other business area Information Assets.

13. IAOs are responsible for ensuring they have a business and information classification process in place for the information received, created, and used within their business areas. They need to identify the key controls required for protecting the information from unauthorised disclosure, alteration or destruction, dissemination or loss and take proportionate measures to ensure that information (in physical and electronic formats) is used appropriately and securely depending on its classification to include:
    - Secure use;
    - Storage;
    - Transmission; and
    - Destruction.

14. They are also responsible for considering any privacy issues at the outset of new implementation or changes to projects, processes or systems which involve the processing of personal data and identify measures to mitigate risks to individuals' privacy rights. A Data Protection Impact Assessment (DPIA) should be completed to identify the privacy risks and to put in place plans to mitigate any identified risks.

Audience

15. The Information Classification Scheme is intended to be read in conjunction with the Information Governance Framework and understood by all individuals who have access to University information and technologies, including external parties that provide information processing services to the University who have been granted access to University information and/or allied information systems and services. (Staff, contractors, third-party suppliers, visitors and students on placement/internship i.e. any person(s) not employed by the University).

16. Requirements should be adhered to and should inform decision making whenever information and information capture systems and processes are reviewed or replaced.

17. This procedure applies to all locations and instances where:
    - the University is responsible for handling/processing activities related to business and personal and/or sensitive personal data as the data controller;
    - Information and/or data over which the University is recognised as the owner are accessed – irrespective of location and the ownership of the technology and the service(s) used to access information and data that fall within the scope of this procedure including all out of office (e.g. home) working.

Definitions

18. All definitions relating to Records Management, Information Governance and Information Compliance are captured in our short guide titled Information Governance Definitions. This includes any terms used in the Information Classification Scheme.

Classification Scheme

Using effective Information Management Systems

19. Business areas need to ensure that there are effective information management processes in place for paper and electronic information processed and held in their areas. This could be managed on one or more computer programmes and held in associated databases. This provides a variety of functions including access controls, auditing and disposal using a combination of system and user generated information.

Using Labels, Descriptors and Filing Structures

20. Business area filing structures should be in place and provide an environment for presenting a common understanding of how information should be stored and retrieved within that business area.

21. Filing structures should be well designed through careful structure of folders (with meaningful titles using naming conventions) containing the information. A well-designed filing structure will allow the business area and therefore the University to control access and enable a meaningful way to manage records and business information and the retrieval of information when appropriate.

22. Information may be marked with a descriptor to identify the reason why a classification is applied and an expiry date if necessary. A descriptor can also be used to show when information also falls within another organisation's classification scheme.

Classification process

23. A business area's classification process should include requirements that determine the initial classification level for that item of information.

24. Where information has been received from a third party and already has a classification, this should be retained, and mapped to the University classification scheme so that the appropriate handling/processing arrangements can be made. Some third parties may specify handling/processing requirements for their information, which should be respected

University information classification levels

25. The University's information classification scheme contains three levels:

    Confidential – Restricted to persons as defined by the Information Asset Owner

    - This means information that, if subject to unauthorised disclosure, alteration or destruction, dissemination or loss could result in serious level of risk to the University, its affiliates or a third party.
    - Authorised access is controlled and authorised by the responsible IAO (or their delegate). Processes are developed to restrict access to groups of people by their job classification or responsibilities (role-based access).
    - A significant level of security controls should be applied to Confidential Information to cover risks.

    Internal – All Staff

    - This classifies information that, if subject to unauthorised disclosure, alteration or destruction, dissemination or loss could result in a moderate level of risk to the University, its affiliates or a third party.
    - Authorised access is controlled and restricted to groups of people by their job classification or responsibilities (role-based access) and constrained by service/department.
    - A moderate level of security controls should be applied to Internal Information.

    Public

    - This classifies information that, if subject to unauthorised disclosure, alteration or destruction, dissemination or loss would result in little or no risk the University, its affiliates or a third party leading to a Minimal Level of Damage.
    - The University has adopted and abides by the model Publication Scheme issued by the ICO. This means that the University commits to making a significant amount of its information publicly available under its Publication Scheme.

26. Where information classified as Internal or Confidential is shared with others for a valid University business reason, everyone should ensure that the recipient is aware of the information's classification and their obligation to protect it. Access to information in these classifications by a third party may require a data sharing or confidentiality agreement in place, signed on behalf of the University and the other party.

Determining the appropriate classification Level

27. The Information Classification Matrix, Appendix A, provides direction on how to classify information, it is important to ensure that the classification process supports consistent classification.

28. A risk-based approach should be followed when determining the appropriate level of classification by evaluation of the risk associated with unauthorised disclosure, alteration or destruction, dissemination or loss. The following factors should be taken into account:

    The harm test – how sensitive is the information? If the information were to be released deliberately or accidentally into the public domain, what level of harm may arise? Is harm hypothetical or more likely than not to occur? What controls are in place to reduce harm?

    Restrictiveness – Too high a marking will incur unnecessary cost and will place restrictions on the use of information. This may mean that applying the handling/processing and management restrictions could impede legitimate uses of the information. Conversely, applying too low a classification may mean that people and the University are placed at risk, where harm arises as a result of the information not being adequately protected.

    The current information lifecycle (draft to finalised documents) – Information classification should be driven by an evaluation of the risk associated with each stage of a document's life cycle. Information contained within draft and/or early concept documents often has a higher degree of sensitivity, notably when there is a free and frank exchange of information, for the purposes of deliberation and decision making. Once a document has been finalised and is ready for distribution to its intended audience (perhaps by a committee or management team following approval) the sensitivity of the information may have reduced, requiring a lower level of classification.

Breaches and Sanctions

29. If the University fails to adhere to its legislative, regulatory and contractual obligations this may result in significant financial and legal penalties including reputational damage.

30. Failure to comply with this procedure could introduce a range of threats to students, staff and University information. Any information security incidents resulting from non-compliance could result in action to be taken under the University's appropriate disciplinary procedure or action been taken by the ICO against the University or against the individuals involved.

31. The University has an obligation to inform the ICO and other effected Data Controllers of any significant information security breach relating to personal data as per DPA 2018 and GDPR. It is also required to inform individuals of any infringements of their information rights.

32. It is therefore vital that everyone reports any observed or suspected information security incidents where a breach of the University's security policies has occurred, any security weaknesses in, or threats to, systems or services.

33. It will be a serious breach where safeguards required for the protection of information classified as CONFIDENTIAL are not put in place or not followed with a reasonable level of care.

34. Where contractual terms have been broken the University will review its position with that party. This could lead to termination of a contract of employment, studies, research or the provision of goods/services.

35. Where it is believed that a criminal action has occurred, the University will also report this to law enforcement agencies. The University also reserves the right to pursue through the Courts a breach of the common law of confidence where it believes that such action is justified. This may also include the pursuit of civil damages against any third party.

References and Associated Documentation (Legislation, Other Policies)

36. Any legal or contractual stipulations surrounding information and/or data created by a third-party, which is received and accepted by the University are to take precedence over the standards and controls set out in this procedure.

37. This procedure needs to be understood in the context of the other policies and procedures constituting the University's Information Governance Framework.

38. Classifying information stipulates how information is to be protected and managed during its handling/processing and use, while the information retains that particular classification.

39. When the corresponding protection controls are followed the likelihood that confidentiality and/or security will be breached should be reduced. Business areas should be able to demonstrate that procedures are in place that reduce the likelihood of unauthorised disclosure, alteration or destruction, dissemination or loss including proactive measures to reduce the likelihood of data breaches occurring.

40. In order to protect information consistently, it is necessary to define a University-wide scheme for classifying (describing) information and identifying how it should be handled according to its requirements for confidentiality, integrity (data quality) and availability. The use of an information classification scheme enables the University to embed good information handling/processing processes in all that it does so that it is clear to everyone with access to know how best to protect it from unauthorised disclosure, alteration or destruction, dissemination or loss.

41. An information classification scheme must be linked to a business classification scheme which describes an organisations business functions and activities, and the relationships between them relative to others:
    a) **Functions** are the largest units of business activity. They are the major responsibilities that are managed by an organisation to fulfil its mission or mandate, and its responsibilities to its stakeholders.
    b) **Activities** are the tasks performed to accomplish each function.

    The linking of both these schemes is an established basis for a functional approach to managing the University's vital records and its Records Retention Schedule. As Information Classification guidance under BS ISO/IEC 27002:2013 Section 8.2 states that: (1) the information should be entered in the Inventory of Assets (control A.8.1.1 of ISO 27001), (2) it should be classified (A.8.2.1), (3) then it should be labelled (A.8.2.2), and finally (4) it should be handled in a secure way (A.8.2.3).

Dissemination

42. The Classification Scheme will be made available to SIROs and IAO's as part of their training and made available to all staff through the Information Governance Guidance Index. The Scheme will be published on the staff intranet and disseminated though the Information Management Operations Group.

Monitoring and Compliance

43. This Scheme will be reviewed by the Head of Information Governance no less than every three years. Any amendments or additions will be submitted to the Information Management Operations Group for approval. The next review is scheduled for July 2023.

LEEDS BECKETT UNIVERSITY

Appendix A – Classification Scheme Matrix

Classification	Public	Internal - All Staff	Confidential
Information/ Information Asset	This classifies information that, if subject to unauthorised disclosure, alteration or destruction, dissemination or loss would result in little or no risk the University, its affiliates or a third party leading to a Minimal Level of Damage.	This classifies information that, if subject to unauthorised disclosure, alteration or destruction, dissemination or loss could result in a moderate level of risk to the University, its affiliates or a third party leading to a Moderate Level of damage.	This means information that, if subject to unauthorised disclosure, alteration or destruction, dissemination or loss could result in significant level of risk to the University, its affiliates or a third party leading to a Serious Level of Damage/Harm.
Risk	***Low*** - This means information that can be disclosed or disseminated without any restriction on content, audience, time of publication as the release of this information would not breach any relevant laws (notably privacy) or a duty of confidence.	*Moderate* - This means information that would not be released into the public domain, without some form of risk evaluation by IAOs/IAAs, to establish that release would not cause any harm.	*Serious* - Where the impact of the risk could harm the University's reputation or have a significant financial effect on the University its affiliates or a third party. Where either personal (or sensitive personal) or internal service configuration or business sensitive data being divulged would equate to the University being at risk from Information Commissioner's Office sanctions.
Security Controls		A moderate level of security controls should be applied to Internal Information.	A significant level of security controls should be applied to Confidential Information to cover risks
Access Controls	Unrestricted access. The University has adopted and abides by the model Publication Scheme issued by the ICO. This means that the University commits to making a significant amount of its appropriately classified public information publicly available under its publication scheme.	Access controls must be observed from creating to destruction. Authorised access is controlled and restricted to groups of people by their job classification or responsibilities (role-based access) and constrained by service/department.	Access controls must be observed from creating to destruction. Authorised access is controlled and authorised by the responsible IAO (or their delegate). Processes are developed to restrict access to groups of people by their job classification or responsibilities (role-based access).

		Authorised access could be provided to a person once they became a taught student or a member of staff at the University (NB this is not the same as 'everyone who has an account' at the University).	Limited to members of the University, partner organisations (where covered by data sharing agreements) and individuals as authorised by IAOs (or their delegate).
User devices	Password protection suggested; locked when not in use	Password protection required (Passwords to be communicated via mechanism separate to sharing the link to the files with colleagues); locked when not in use. Encryption suggested.	Password protection required (Passwords to be communicated via mechanism separate to sharing the link to the files with colleagues); locked when not in use. Encryption required.
Disposal (for additional detail, see short guide of Disposal – Risk)	Recycling	Irreversible destruction Cross-shredding Incineration Use of certified contractor	Irreversible destruction Cross-shredding Incineration Use of certified contractor
Retention	All Information must be retained for the legally or contractually required minimum and maximum periods of time as per local retention requirements, the University Records Retention Schedule and the JISC HE Business Classification. This will vary on the type of information under consideration.		
PERSONAL INFORMATION – As defined by the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018). (Please see the University's Data Protection	**Public/ Information Assets may include but are not limited to:** Anonymised information - information which cannot identify an individual either in isolation or when combined with other information (Article 4, GDPR). (NB Anonymised data may also carry other handling requirements) Staff Details shared publicly by the University	**Internal/ Information Assets may include but are not limited to:** Staff Names Staff Work Contact Details (including job titles) Student Names and Email addresses Academic Staff Qualifications and Publication Details	**Confidential Information/ Information Assets may include but are not limited to:** Personal data; home address, personal contact details, NI number, age, individual's image (including CCTV footage) Staff appointment, promotion or details of personal affairs, employee contract information, wage slips, passports, driving licences, death certificates and non-disclosure agreements.

Policy) **Examples (non-exhaustive)**	Information on individuals made public with their consent including on social media sites or departmental websites	ID number Online identifier (social media sites) Location data IP address Mobile phone number	Student registration and attendance details, exam scripts, marks, comments on student performance, student academic progression, provisional degree classification prior to formal approval and any publication Sensitive personal data; data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; and the commission or alleged commission by them of any criminal convictions or offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. Biometric data e.g. fingerprints, facial recognition. Financial information relating to individuals e.g. banking information, salary details, indebtedness (student fees) Grievance/disciplinary proceedings References for staff or students UCAS forms
		Dates of birth (DoB)	Individual’s name plus DoB or other personal data; national insurance number (NI), passport details, home address. Adding additional combinations of data can change the overall classification (sensitivity) of the information. Increasing the volume can also increase the classification level. For further detail see the

			procedure for managing and reporting information breaches.
NON-PERSONAL Information **Examples (non- exhaustive)**	Anything subject to disclosure under the Freedom of Information Act 2000 (FOIA) Department and Course details Marketing or Press Information Factual and general organisational information for public dissemination including annual reports or accounts Public events	HR Policies and Guidance	Information relating to supply or procurement of goods/services prior to approved publication Research Proposals prior to award - Content dependent 'Trade' secrets, intellectual property intended for commercialisation Research Data which is security-sensitive or has been similarly classified by an external body (e.g. Government, commercial partner with a confidentiality agreement) Research papers intended to lead to patentable results (If research is on-going and has not been published) Details of servers and server rooms Passwords Exam Papers Non-Personal Information which is security-sensitive or has been similarly classified by an external body Commercial Contracts - University and third-party contract/supplier information Correspondence with Police, Legal Counsel/Legal advice or other information relating to legal action against or by the University Market sensitive information