Organisation	Oxford Brookes University
Title	Information Classification Policy
Creator	Information Security Team
Approvals required	CIO; VCG
Version	1.0
Owner	Head of Information Security Management
Subject	Information Security Management
Rights	Public
Renewal date and responsibilities	Annually by the Information Security Working Group. Drafted on 9 October 2018

Revision History			
Date	Author	Version Number	Comments
09/10/18	Kate Phizackerley	0.1 (draft)	Original draft
31/03/19	Gareth Packham	1.0 (live)	Minor revisions only

1. Purpose

This policy establishes a framework for classifying work-related information (information) in order to:

- promote the safe transmission and sharing of information with legitimate parties.
- reduce the risk of harm to the confidentiality, integrity and availability of information processed by or on behalf of the Oxford Brookes University.
- advance the University's compliance with ISO 27001:2013 standards (Clause 7.2.1).

2. Scope

This policy covers all types of handling, sharing (processing) and storage of information, including teaching, research, commercial and non-commercial activities as well as administration carried out directly for the University, any affiliates or partners, or by the University on behalf of another organisation.

There is a separate guidance policy for security sensitive material.

The Oxford Brookes University Information Classification Policy will apply to either an instance or regular information sharing, save where the law or other written agreement provides otherwise.

3. Information classification

(Examples of how to apply the classification markings are found at 5. below and Appendix 1.)

All information falling within the scope of the policy must be classified in accordance with the following categories: 'Confidential'; 'Restricted'; and 'Public'.

The following classifications are generally available for application:

Confidential:
This information has a significant value for Oxford Brookes University, another organisation or individual. Wrongful disclosure could impact the reputation or standing of an organisation or an individual, the safety of an individual or could cause significant financial loss. Information of this type is shared on a "need to know basis" only. This classification will include Special Category of Personal Data as defined in Data Protection Law (see Appendix 1). Large amounts of datasets of information which would otherwise be classified as "Restricted" were it a smaller amount, may become classified as "Confidential" by merit of the quantity of data involved. If in doubt as to whether a dataset is large, query this with the Information Security team by email using info.sec@brookes.ac.uk

Restricted: This information can be shared appropriately with a limited audience, usually but not exclusively within the University. Some of the features attributed to "Confidential" information
apply, yet the implications associated with sharing this information are less serious. This information could be financial or commercial value, or be subject to intellectual property, trademark or other legal protection. It would be likely to include emails and document containing personal data.

Public (or unclassified): This information can be readily shared and publically available. It could be on the Oxford Brookes University website with no adverse consequences for any organisation or individual.

4. Responsibility for classifying information

Anyone who is the author of information, or involved in processing information is responsible for ensuring that it is appropriately classified. Should anyone receive information which is not classified as it should be, that recipient becomes responsible for ensuring that any information is classified at that stage, in consultation with the relevant data owner.. This can be achieved either by reverting to the source or by classifying it on receipt, whichever is appropriate in the circumstances.

5. Guidance

5.1 How to apply the classification marking

Consider all relevant factors when classifying documents which are set out in the respective classifications and examples in Appendix 1 and apply the appropriate classification marking: Confidential, Restricted or Public.

5.2 Transmitting and sending information

Please apply the Information Sharing and Transmission Policy when transmitting or sending information found at www.brookes.ac.uk/it/information-security/policies-procedures-legislation

5.3 The storage and retention requirements

Any documents or data must be classified whether saved digitally or stored manually. (It is good practice for a document or data to contain a date, as well, to facilitate applying the Retention Policy.)

Any document or data which is classified as "Confidential" or "Restricted" must be handled in accordance with the Oxford Brookes Information Handling Guidelines.

Appendix 1

Examples of how to classify different types of information are included in this table. This list is neither exhaustive nor prescriptive, it is included as an aid.

Confidential	**Restricted**	**Public**
Interviewee applications (including references)	Research prior to publication	Material which can appear on the Brookes website
Human Resources records for staff	Personal Data (information which identifies or leads to identifying an individual, including email addresses or financial information.)	Published research
Occupational Health Records	Financially or commercially sensitive information such as certain procurement exercises or planning.	Course prospectus
Disciplinary Records	Restricted policies (eg parts of the Business Continuity Plan, security procedures etc.)	Policies, Guidance and Procedures (save when restricted)
Some student information (confidential addresses etc.)	Student contact information (save where it is confidential.)	Annual accounts once formally released for publication.
Staff information (confidential email addresses etc.- likely to be on Human Resources file anyway).	Preparatory work for Annual Accounts	Faculty and staff directory information
Special Category Data such as racial/ethnic origin, political opinion, religious beliefs, Trades Union Membership.	Minutes of meetings where the discussion was not about a confidential matter.	Salary ranges (not individuals' salaries, generally) Annual accounts
Individuals' Bank details		
University bank details		
Information about Criminal Convictions and/or DBS checks		
Large amounts of Personal Data are deemed to be		

Confidential because of the quantity of records. Minutes of confidential meetings, or any section of minutes which are confidential.		

Appendix 2

Additional Factors to consider when classifying information

- Where information is **not classified** and is not in the public domain already it should be treated as “Confidential” and afforded the highest levels of protection pending classification.

- Where information is held, handled or shared regularly or there is a large amount of data being processed either by or on behalf of another organisation, a contract or Information Sharing Agreement should cover the processing. This document is a legal requirement. It should set out which organisation’s Classification Policy applies (as well as covering other issues).

- Certain professions or functions have a regulatory body which stipulate how work-related information must be handled (e.g. occupational health, social services, research). In the unlikely event of any conflict within this policy and any guidance from a professional body, please raise this with the IT Services Information Security team by email using info.sec@brookes.ac.uk

- Where material contains characteristics of more than one classification, the entire document or all data is afforded the most protective marking.

- Databases or stored information classified as containing “Public” information must not contain any “Restricted” or “Confidential” information, except where the confidential parts have been redacted, or protected. The Restricted or Confidential information must be unavailable. This redaction can be achieved by e.g pseudonymisation de - identification, anonymisation or obfuscation.

- Any restricted or confidential elements of the information must be stored separately and given the relevant classification and protection relevant to their content.

- The classification of information may change over its lifespan, as its value to the University or to an individual changes.