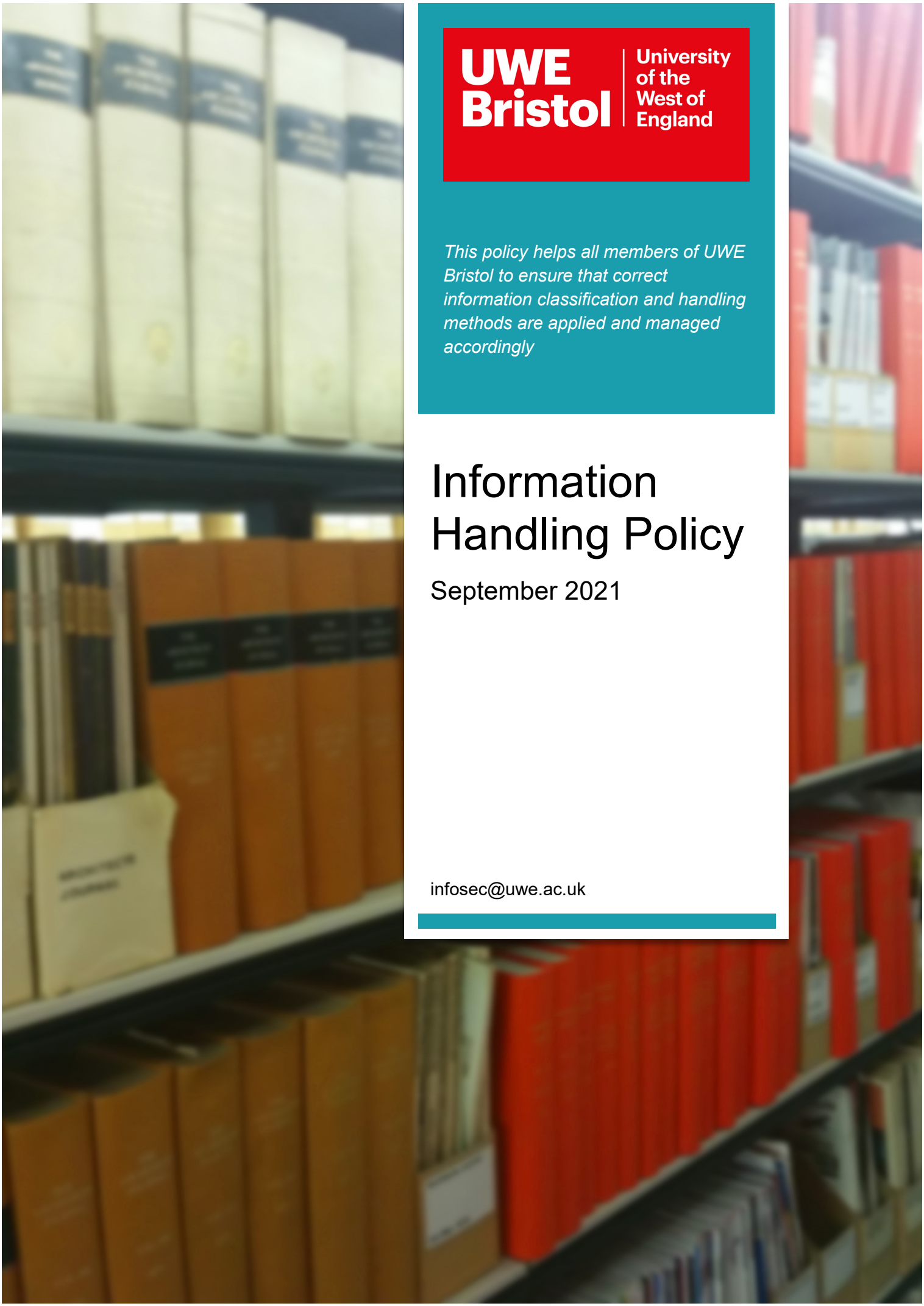

UWE Bristol | University of the West of England

This policy helps all members of UWE Bristol to ensure that correct information classification and handling methods are applied and managed accordingly

Information Handling Policy

September 2021

infosec@uwe.ac.uk

Document Control

Writers & contributors	Head of Information Security, Information Security Specialist & Head of Data Protection
Policy owner	Head of Information Security
Publication date	September 2021
Date of next review	September 2022
Version	3.0

Contents

1. Purpose

The purpose of this policy is to seek to ensure staff and students understand how information in their possession should be protected, and how information should be shared with other parties. UWE Bristol generates and holds a wide variety of information that must be protected against unauthorized access, disclosure, modification, or other misuse. Different types of information require specific security measures, and therefore proper classification of information assets is vital to ensure effective information security and management practices are adhered to across the University.

This document forms part of the Information Security Policy Toolkit and underpins the overarching Information Security Policy. Adherence to this policy will provide everyone with guidance to help ensure that correct information classification and handling methods are applied to their day-to-day activities and managed accordingly.

2. Scope

This policy applies to all information assets generated or processed by UWE Bristol, including those created prior to the publishing of this policy. This includes electronic information as well as information on paper and information shared orally or visually (such as telephone and video conferencing). Where UWE Bristol holds information on behalf of another organisation with its own classification system, agreement shall be reached as to which handling policy shall apply.

3. Responsibility

It is the responsibility of UWE Bristol to ensure that adequate data storage and processing facilities are available to enable compliance with the Information Handling Policy. Individuals have a personal responsibility to ensure the correct management and protection of information, and may be personally liable for any breaches in information security that arise from a failure to take appropriate measures to do so.

4. Consequences of Policy Violation

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply may lead to the immediate cancellation of a contract. Where appropriate, breaches of the law will be reported to the authorities.

5. GDPR

UWE Bristol must comply with data protection law(s). Failure to comply with data protection law(s) and any subsequent data breach(es) can cause significant distress to individual and can result in large fines and other legal sanctions/regulatory enforcement action. This may adversely affect the University's relation with key stakeholders (e.g. current and prospective students) as well as the University's reputation. In addition, deliberate misuse of personal data is also a criminal offence for which you can be held personally liable for.

Understanding how information in your possession should be protected and how it should be shared with other parties when it contains personal data will help you comply with some aspects and principles of UK data protection law(s). You may find it helpful to refer to the University's Data

Protection Policy in order to understand the definitions of personal data as well as the other measures/action you should take when complying with UK data protection law(s).

6. Information Classification

All information generated or processed by UWE Bristol is subject to classification. This is to assist information owners in determining the different levels of security required. The following classifications are used by UWE Bristol:

UWE Public	Information that is available to any member of the public without restriction. This however should not be automatically placed into the public domain without a specific reason, unless the information was originally intended for public disclosure
UWE Internal	Non-confidential information where dissemination is restricted to specific groups or individuals for policy, operational or contractual reasons, for example: some committee minutes; procurement documents; or internal reports. Typically, if this level of information was leaked outside of the University, it could be viewed as inappropriate or ill-timed
UWE Confidential	Information which contains personal data of others will also need to be handled in accordance with UK data protection law(s) and the University's Data Protection Policy. Whenever personal data is involved careful considerations needs to be given to its classification. It is conceivable that information containing personal data can fall into any of the UWE classifications. As a general rule, information which contains sensitive data (e.g. special category data) will fall into the "UWE Confidential" category. In some circumstances, personal data that is not of a sensitive nature (e.g. not special category data) that has been appropriately pseudonymised and/or subject to appropriate security controls, may fall into the "UWE Internal" category (e.g. some meeting minutes). In these circumstances, UK data protection law(s) will still apply, and this information still needs to be handled in accordance with the University's Data Protection Policy.

Occasionally, information which contains personal data can sometimes fall into the "UWE Public" category if UK data protection law(s) is appropriately complied with. In these instances, you should first seek the advice of UWE's data protection office (dataprotection@uwe.ac.uk) before classifying information which contains personal data as "UWE Public".

7. Management of Information

Each department or service must hold a full inventory of all Confidential information assets. Each asset will have an accountable owner, and although responsibility for the security measures may be delegated to a named individual, accountability remains with the owner. Owners should always have an Information Management Plan in place, which will detail the storage, access and retention arrangements of the information in question. This will ensure that consideration is given to how data will be handled across its lifespan, including whether all data or parts thereof need to be archived, made available for further use by others, or securely disposed of. The Information

Management Plan is a key component of the Information Management Strategy, which provides guidance on Information Management principles and best practices.

8. Storage of Information

Information of any classification should not be stored locally on workstations or laptops. Instead, information should be saved to file systems managed or provided by UWE IT Services, such as SharePoint or OneDrive. Procedures governing the storage of information must be in place based on the nature of the document. For paper files, this may include locking the document away when not in use. When printing or copying any confidential data, the device or printer must be physically secure or attended. Archived or legacy information that does not meet the storage requirements below should be reviewed and made compliant at the earliest appropriate opportunity.

UWE Public	• Electronic information should be stored using UWE provided IT facilities where possible to ensure appropriate management, back-up and access
UWE Internal	• Electronic information must be stored using only UWE provided IT facilities
UWE Confidential	• Electronic information must be stored using only UWE provided IT facilities • Storage locations must be appropriately access controlled (locked cabinets for paper documents and filesystem/access permissions for electronic data) • Removable media, such as USB drives, should only be used, with justification, where UWE provided file systems are not accessible. Files must be encrypted to mitigate the risk of devices being lost or stolen. • ITS provided OneDrive is the only cloud storage permitted for use

9. Disposal of Information

Retention periods for information held must be determined in advance by the owner, according to the business need and recorded in the University's Retention Schedules. Please contact your Data Protection Coordinator and the Data Protection Office (dataprotection@uwe.ac.uk) in order for the appropriate changes/additions to be made. Generally, information should not be kept longer than it is required for business use (the retention period will be defined in the retention schedule), unless required for archival purposes or to satisfy contractual or statutory obligations. You may find it helpful to refer to the University's Records Management policy for more information.

UWE Public	• Electronic information may be deleted using regular file deletion processes in accordance with any retention schedule. Paper documents should be disposed of via the paper recycling scheme and in accordance with any retention schedule
UWE Internal/ UWE Confidential	• Electronic equipment holding this information must be disposed of using the UWE secure IT waste disposal service in accordance with any retention schedule • Paper documents should be disposed of via the UWE secure waste disposal service in accordance with any retention schedule

10. Dissemination and Exchange of Information

When sharing information, the appropriate method of transfer must be decided, taking into account the nature and volume of the information being exchanged and the impact of inappropriate disclosure. Intended third party recipients of information or documents must be authorised to receive such information and have sufficient information security policies and procedures in place to assure the confidentiality and integrity of the information.

When sharing and/or transferring information that contains personal data, appropriate measures need to be put in place with the organisation/individual you are sharing and/or transferring personal data with/to. Generally, this includes a Data Processing or Data Sharing agreement. If you need to share and/or transfer personal data externally and are unsure as to whether the appropriate measures are already in place with the organisation/individual, please contact the Data Protection Office (dataprotection@uwe.ac.uk) for further assistance.

UWE Public	• Electronic information can be exchanged via email or file sharing without requiring encryption
UWE Internal/ UWE Confidential	• Electronic Information must be encrypted and only shared using UWE provided IT facilities e.g. SharePoint, OneDrive • Information must be marked 'UWE Confidential' where appropriate and the intended recipients clearly indicated • Duplicate copies of UWE Confidential information should be avoided. Where copies are necessary, the 'UWE Confidential' marking must be clearly indicated on the copies. Where paper copies are required for sharing, secure delivery methods must be used, and arrangements for disposal confirmed in advance