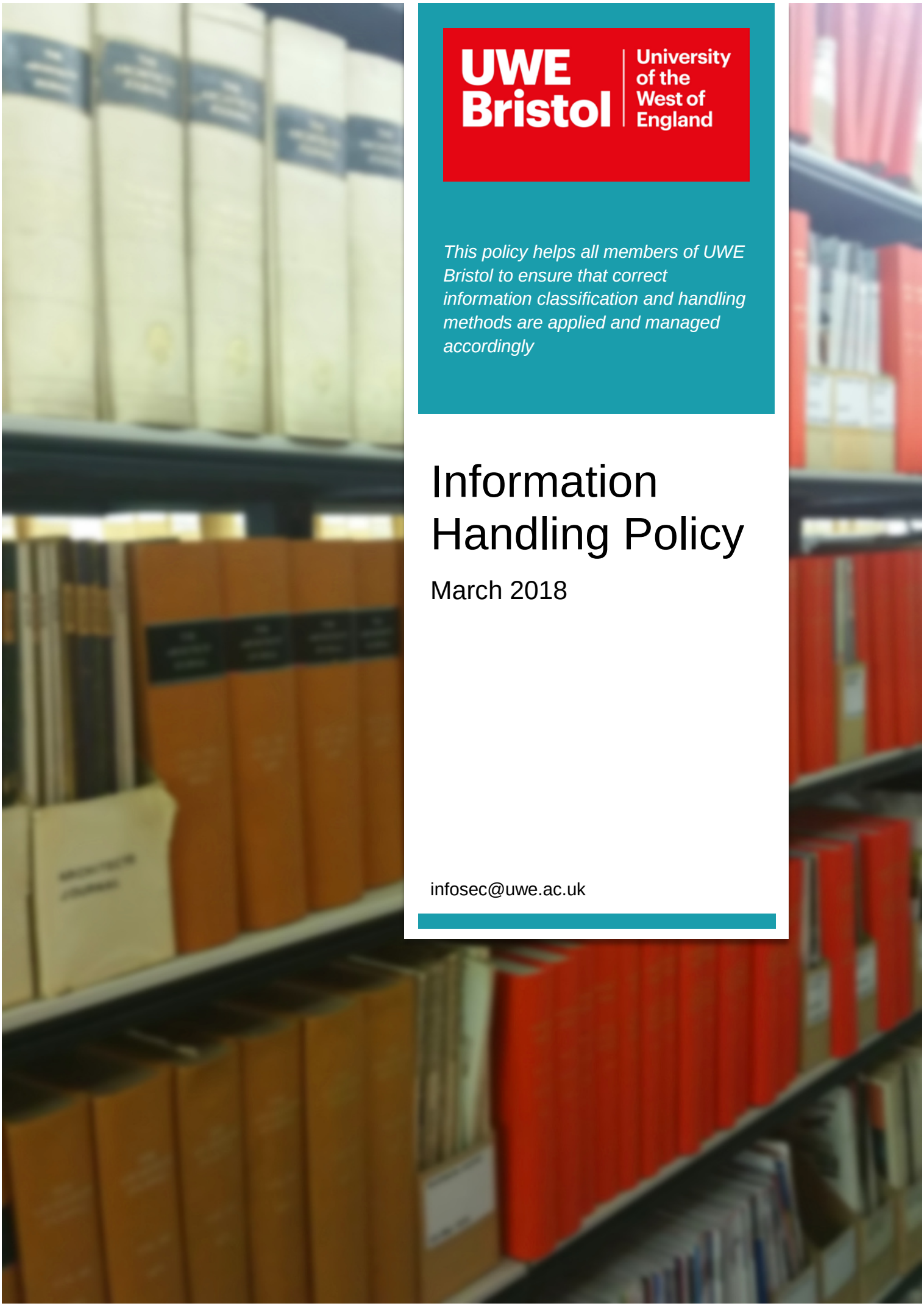

UWE Bristol | University of the West of England

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

March 2018

infosec@uwe.ac.uk

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

Failure to comply with data protection means the University is breaking the law. This can result in large fines and other legal sanctions. Data breaches can also cause significant distress to individuals and have an adverse impact upon the University's reputation with the media and other key stakeholders such as prospective students. Deliberate misuse of personal data is also a criminal offence for which you can be personally liable.

Personal data is any information attributable to an identifiable individual, including names and email addresses. For example, details of a student’s academic performance and qualifications constitute personal data.

Sensitive personal data ("special categories" under GDPR) includes disability status, ethnicity, medical information (both physical and mental) and details of criminal convictions, and may require heightened security measures such as encryption and stricter access controls.

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:

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
Restricted	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
Confidential	Information which requires additional protection because it is sensitive personal data, commercial or legal information, under embargo prior to wider release, or which could not be disclosed under Freedom of Information legislation

Except for information which is obviously and legitimately in the public domain (such as job titles and departments), personal information (as defined in the Data Protection act) will, as a general rule, fall into the Confidential category.

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 filesystems managed or provided by ITS, such as the H or S drives, 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.

Public	• Electronic information should be stored using UWE provided IT facilities where possible to ensure appropriate management, back-up and access
Restricted	• Electronic information must be stored using only UWE provided IT facilities
Confidential	• Electronic information must be stored using only UWE provided IT facilities • Portable devices must have full disk encryption • Storage locations must be appropriately access controlled (locked cabinets for paper documents and filesystem/access permissions for electronic data) • Unencrypted removable media (eg USB drives) must not be used. Encrypted removable media is not permitted without justification and evaluation of other options • ITS provided OneDrive is the only cloud storage permitted for use and in all cases data must be suitably encrypted

9. Disposal of Information

Any paper documents with a classification of 'Restricted' or above must be shredded. When disposing of equipment containing storage media, all data must be irretrievably deleted as described below. Retention periods for information held must be determined in advance by the owner, according to the business need. Information should not be kept longer than it is required for business use, unless required for archival or to satisfy contractual or statutory obligations.

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
Restricted / 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 • Large accumulations of data should not be downloaded or copied

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. Confidential information may only be transferred across external networks, or copied to other media, once it has been encrypted and password protected. If the Confidential information contains personal data, then transfer to external organisations must only occur if a UWE Data Processing Agreement

is in place with that organisation. Email addresses should be checked prior to dispatch, with particular regard to any auto corrections, especially where the information content is sensitive.

Public	• Electronic information can be exchanged via email or file sharing without requiring encryption
Restricted	• Electronic information can be exchanged via email without requiring encryption • Electronic information can be shared using UWE IT facilities (eg SharePoint, OneDrive)
Confidential	• Electronic Information must be encrypted and only shared using UWE provided IT facilities • Information must be marked 'Confidential' and the intended recipients clearly indicated • Duplicate copies of Confidential information should be avoided. Where copies are necessary, the '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