University of Bristol
Information Security Policy - Information Handling

Title	Information Handling
Reference	ISP-07
Status	Approved
Version	3.0
Date Created	July 2013
Last Reviewed	October 2023
Next Review	October 2024
Classification	Public

Contents

1. Introduction

This Information Handling Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the requirements relating to the handling of the University's information assets. Information assets must be managed in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation that would otherwise occur.

2. Scope

Members of the University (as defined in University's Constitution: Ordinance 9, section 7), members of other institutions who have been granted access to University information assets, together with any others who may have been granted access to University information assets are subject to this policy.

Generated research data is governed by:
https://www.bristol.ac.uk/research/environment/governance/research-data-policy/.

3. Policy

3.1. Inventory and Ownership of Information Assets

The University maintains information asset registers detailing its main information assets and assigning ownership to information asset owners. Each asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

3.2. Security Classification

Each information asset will be assigned a security classification by the asset owner. This security classification will reflect the sensitivity of the asset according to the following classification scheme:

- Public – available to any member of the public without restriction.
- Open – available to any authenticated member of the University.
- Confidential – available only to specified members, with appropriate authorisation.
- Confidential and Sensitive – available to only a very small number of members, with appropriate authorisation.
- Secret – the most restricted category. Available only to a limited and defined number of authorised members and may have additional document handling and access requirements.

Any information that is disclosable under the Freedom of Information Act 2000 will be classified as public.

Any personal data that is classified as special category data under the Data Protection Act 2018 (or its successor legislation) will be classified as confidential and sensitive.

Any data that is subject to the Official Secrets Act 1989 will be classified as secret.

Any information that is not explicitly classified in accordance with the University's data classification scheme and the examples therein should be handled as Confidential by default.

University Information Classification Scheme: Information Security Classifications.pdf (bristol.ac.uk).

Guide to legislation relevant to Information Security Policy: guide.pdf (bristol.ac.uk).

3.3. Access to Information

Members of the University will be granted access to the information they need in order to fulfil their roles within the University. Members who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

3.4. Disposal of Information

Information assets must be disposed of with care in accordance with classification requirements.

Paper waste that is classified as Confidential or above must be disposed of following formal University procedure.

University Confidential Waste Procedure:
https://uob.sharepoint.com/sites/sustainability/SitePages/Confidential.aspx

Electronic information must be securely erased or otherwise rendered inaccessible before leaving the possession of the University, unless the disposal is undertaken under contract by an approved contractor.

In cases where a storage system (for example a USB stick, portable drive or printer hard drive) is required to be returned to a supplier, it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of the University until it is disposed of securely.

3.5. Removal of Information

University data subject to the Data Protection Act or that has a classification of Confidential or above must be stored using University facilities or with third parties subject to a formal, written legal contract with the University. In cases where it is necessary to otherwise remove data from the University, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Information classified as Confidential or above in electronic form must be securely encrypted, as instructed in the University's Encryption Standard, prior to removal or transmission. Secret data must never be removed except with the explicit written permission, and in accordance with the directions of, the data owner.

3.6. Using Personally Owned Devices

Any processing or storage of University information using personally owned devices must comply with the University's Mobile and Remote Working Policy (ISP-14).

3.7. Information on Desks, Screens and Printers

Members of staff who handle paper documents containing information classified as Confidential or above must take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Documents classified as Confidential or above must be locked away overnight, at weekends and at other unattended times.
Care must also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which information classified as Confidential or above is processed or viewed must be sited in such a way that they cannot be viewed by unauthorised persons.

All computers must be locked while unattended.

3.8. Backups

Information asset owners must ensure that appropriate backup and system recovery measures are in place and that those measures are compliant with any agreements with external partners from whom data has been obtained.

For all backups, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

3.9. Exchanges of Information

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.
Information classified as Sensitive and Confidential must be strongly encrypted prior to electronic exchange, both within the University and in exchanges with third parties. Information classified as Secret may not be transmitted electronically except with the explicit written permission of the information owner and in accordance with their handling requirements.

When exchanging information by email, SharePoint, fax or other digital information sharing methods, recipient addresses should be checked carefully prior to transmission.

When exchanging data classified as Confidential or above over email, the use of Bcc should be avoided. For further guidance see the ICO guidance on Email and security | ICO.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information that is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Members of the University must not disclose or copy any information classified as Confidential or above unless they are authorised to do so.

3.10. Reporting Losses

All members of the University have a duty to report the loss, suspected loss or unauthorised disclosure of any University information asset to the information security incident response team (cert@bristol.ac.uk). This includes the loss of personal devices, such as phones or USB drives, on which University information assets might reside.

For information about how to manage incidents involving personal data, visit:
www.bristol.ac.uk/secretary/data-protection/data-breaches-and-incidents/

4. Further Guidance

- Mobile and Remote Working Policy (ISP-14)
- UoB Data Classifications
- Confidential Waste (sharepoint.com)
- Disposal of Computer Equipment
- Personal Data Breach Procedure