UHI | INVERNESS

Information Transfer Policy

PL/IT/2025/001

Lead Officer	ICT Services Manager
Review Officer	Information Development Manager
Date first approved by BoM	December 2024
First Review Date	December 2027
Date review approved by BoM	
Next Review Date	December 2027
Equality impact assessment	November 2024
Further information (where relevant)	

Reviewer	Date	Review Action/Impact
ICT Services Manager	25/09/24	Policy created and approved.

Contents

1. Policy Statement

Information is stored and maintained in systems for specific purposes and with specific access rights. In every transfer of information, both within the College and with external parties, there is a risk information could be lost, misappropriated, or accidentally released beyond its necessary audience.

The purpose of this policy is to outline the restrictions on transferring information to ensure the security of information, particularly personal data, is maintained.

The Information Transfer policy is part of the wider UHI Inverness Information Security Management System (ISMS).

2. Legislative framework / related policies

2.1. UHI Inverness Information Security Policy
2.2. UHI Inverness Information Security Management System
2.3. UHI Inverness Data Protection Policy
2.4. UHI Inverness Records Management Policy
2.5. UHI Partners Acceptable Use Policy
2.6. UK General Data Protection Regulation (UK GDPR)
2.7. UK Data Protection Act 2018

3. Data Principles

3.1. Personal data shall be:
- 3.1.1. processed lawfully, fairly and in a transparent manner;
- 3.1.2. collected for specified, explicit and legitimate purposes;
- 3.1.3. adequate, relevant an limited to what is necessary;
- 3.1.4. accurate and where necessary kept up to date;
- 3.1.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed;
- 3.1.6. processed in manner that ensures appropriate security of the personal data;

4. Scope

4.1. The scope of this document policy is to ensure that staff are aware that any transfer of information should maintain its confidentiality, integrity, and availability. For the purpose of this policy, information includes data stored on computers (including mobile devices), transmitted across networks, printed out or

written on paper, sent out by fax, stored on disk or tape, or, spoken in conversation or over the telephone, including voicemail & video recordings.

5. Definitions

5.1. **Information** is defined as any data, records, documents, or other forms of knowledge created, processed, stored, or transmitted within UHI Inverness.

5.2. **Transfer** is defined as the movement of information from one location to another, including electronic, physical, or verbal transfer. Such as SharePoint content to an email attachment, moving a file to another Cloud storage outside UHI, printing content from the student information system and or sharing data with third party organisations (including contractors and sub-contractors).

5.3. **International Transfer** involves transmission of data to a country outside of the EU. Data protection and security arrangements for countries outside of the EU are not as stringent as required by the EU and UK GDPR. Therefore, we must comply with Articles 45-50 of the UK GDPR when considering international transfers.

6. Responsibilities

6.1. **The information owner** is responsible for the data being transferred. They must identify the sensitivity and classification of any data to be transferred, as well as ensuring a secure mode of transfer. Data should not be shared with any 3rd Party without a data sharing agreement being in place. The information owner is responsible for liaising with the Data Controller to seek advice prior to transfer of data, especially for any new processes, or unusual request for the transfer of data.

6.2. **All staff** should be aware that they should not transfer data, particularly sensitive data, without following a process provided by, or guidance on a one-off action, from the information owner.

7. Methods of Information Transfer

7.1. **Electronic transfer** – data should be transferred using encryption and specific services, such as UHI Dropbox, created for this purpose.

7.2. **System upload** – upload of data via a secure login to an external portal or cloud storage.

7.3. **System processing** – procurement of IT systems or software packages should include a GDPR assessment to assess the level of data security and the country in which the data is stored. This may involve international transfer for back-up purposes.

7.4. **Paper transfer** – by default, personal data should not be printed. Where the information is only needed temporarily, it should be recycled in confidential waste to ensure it is shredded.

7.5. **Verbal transfer** – information that is processed by staff, particularly personal data, is restricted. This restriction should be maintained and not discussed outside of these restrictions.

8. Guidelines and Principles

8.1. Staff should not assume someone is entitled to receive information just because they request it (irrespective of their position within the organisation). It is your responsibility to check whether the sharing of data is valid before releasing it.

8.2. Information must not be shared with 3rd parties without a data sharing agreement or contract being in place.

8.3. Information shared must be limited to what is necessary for the purpose (see data principles). Care must be taken when working with spreadsheets. Spreadsheets containing hidden columns or pivot tables should not be shared. Good practice is to always extract the relevant information and send in a new document.

8.4. Personal data shared must be limited to the necessary data fields. Where possible, data must be anonymised.

8.5. If in doubt about sending personal data, escalate to your line manager or the Data Controller.

8.6. Personal data must not be transferred outside of the college and /or UHI network without the permission of the college Data Controller. This includes emailing data, sending in written form, moving data to another system or storage method or saving to an external drive, such as USB pen drive.

8.7. Personal data should not be moved to another location even within current storage method, such as SharePoint, as it may not be subject to the same permission controls in place.

8.8. Personal data should not be disclosed over the phone without confirming the identity and authority of the recipient.

8.9. Personal identifiable information should not be openly discussed if you have any concerns about being overheard.

9. Compliance

9.1. This policy is a cross-wide college policy; and all staff must work to meet the requirements outlined within the policy. Non-compliance should be reported the Data Controller to mitigate any impact and escalate accordingly.

9.2. events in issuing personal data and / or confidential information to an unintended recipient must be reported to the College Data Controller to allow an Information Security Incident to be raised.

10. Monitoring

10.1. This college policy will be monitored, and its implementation evaluated against data loss and incidents that are a result of not following the information contained within.

10.2. Breaches of data or exposure of data outside intended audiences is reported by the Data Controller to the college executive team monthly, or immediately where it requires more urgent escalation e.g. being reported to the Information Commissioner's Office.

11. Review

11.1. This policy will be reviewed every 3 years.