Information Transfer Code of Practice

Executive Summary

The purpose of this Information Transfer CoP is to establish a framework for the secure transfer of information within and outside the university. By adhering to this CoP, the university aims to protect its information assets, uphold its reputation, and ensure the trust of its stakeholders, including students, staff, partners, and the wider community.

These principles must be adhered to by all users to;

- ensure that the University complies with its legal and statutory obligations,
- protect the confidentiality, integrity and availability of information and systems during transfer processes, and
- provide authorised users of university IT with a safe and acceptable working environment.

CoP Statement

1. The ability transfer information securely is fundamental to the University being able to operate. By implementing this CoP, the university seeks to ensure that information is protected from unauthorised access, disclosure, alteration, and destruction during transfer.

2. By facilitating the efficient and secure transfer of information necessary for academic, administrative, and research activities, the University will ensure that information is accessible to authorised users when needed.

Purpose

3. The purpose of this document is to ensure the security of information when exchanged within or outside the university. Without clear guidance the likelihood of a compromise resulting in economic, reputational or operational damage, both business and personal, would be unacceptably high.

Scope and Application

4. This CoP applies to all information owned by the University or for which the University has a responsibility to protect, including digital, hard-copy, and verbal.

5. This CoP applies to all staff, students, contractors, and third parties who process information owned by the University or for which the University has a responsibility to protect.

6. All applicable users are required to familiarise themselves with this CoP and comply with its requirements.

7. Failure of university users to comply with this CoP may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances, legal action may be taken.

8. Failure of other users to comply may lead to revocation of access, the cancellation of a contract and, in certain circumstances, legal action.

9. Completion of the University's Cyber Security Training module is required by all users to support the effective implementation of this CoP.

Standards

10. Use of the University IT Environment is subject to law and regulation, and the University seeks to ensure compliance with these via this CoP.

11. The CoP also supports adherence to standards required for University PCI DSS accreditation (this being the technical and operational requirements for processing credit card data) and Cyber Essentials (this being a standard for information security).

DEFINITIONS

12. University IT Environment - includes all servers and clients, network connectivity, systems and application software, internal and external services, data, and other computer subsystems and components that are owned or provided by the University, or which are under the University's responsibility.

13. Assets – Includes physical items and information in all forms.

14. University User – any individual afforded access to the University IT Environment via a direct relationship with the university e.g. students, members of staff, academics, associates.

RESPONSIBILITIES

Responsibilities and application of the CoP

15. The Vice Chancellor is responsible for ensuring that the CoP is implemented and maintained, and for ensuring all necessary resources are available to support this.

16. The Director of Digital Services is responsible for operational coordination of the CoP.

17. The Director of Digital Services is responsible for ensuring appropriate policies, procedures, guidance, advice, and training are in place to support the CoP's implementation and compliance, and for ensuring these artifacts are regularly reviewed at appropriate intervals.

References and Associated Documentation (Legislation, Other Policies, other parties)

18. This CoP forms part of a suite of related Information Security documents.

OPERATIONAL APPLICATION

Information Classification

19. All information must be classified according to its sensitivity and criticality.

Transfer Methods

20. Information must be transferred using secure methods appropriate to its classification.

21. Acceptable methods for transferring electronic information include university-approved; encrypted email; secure file transfer protocols (SFTP); encrypted internet connection; cloud services; and encrypted external storage devices.

22. Approved methods for transferring physical information include recorded mail or secure courier services, and hand delivery to an authorised recipient.

Encryption

23. Sensitive digital information must be encrypted during transfer.

24. Encryption standards must comply with university guidelines and industry best practices e.g. non-deprecated versions of TLS for transfer over the internet.

Access Control

25. Access to information must be restricted to authorised personnel only. Authorisation levels must be based on the principle of least privilege.

26. Multi-factor authentication (MFA) must be used for accessing sensitive digital information. Exceptions with compensating controls must be authorised by Head of Cyber Security and Information Governance.

Third-Party Transfers

27. Third parties must comply with university information security policies. This includes contractors, partners, and service providers.

28. Before transferring information to third parties, data sharing agreements must be in place to outline the responsibilities and security measures required to protect the information.

Monitoring and Logging

29. Transfers involving sensitive information must be logged to provide an audit trail. Logs should include details such as the date, time, sender, recipient, and method of transfer.

30. Logs must be retained in accordance with the university's data retention CoP.

Incident Management

31. Any security incidents related to information transfer must be reported immediately via the University incident reporting process.

32. Incident response procedures must be followed to mitigate risks and prevent recurrence.

COP MANAGEMENT

Dissemination

33. Managers must ensure that all users who process information owned by the University, or for which the University has a responsibility to protect, are familiar with this CoP.

34. Completion of the University's Cyber Security Training module is required by all users to support the effective implementation of this CoP.

Monitoring

35. This CoP will be provided to all new and existing staff, students, and members of the University. All other users of the University's IT Environment systems shall be advised of the existence of this CoP, which shall be made available to them.

36. All users are required to familiarise themselves with this CoP and comply with its requirements.

37. Failure of University users to comply with this CoP may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances, legal action may be taken.

38. Failure of other users to comply may lead to revocation of access, the cancellation of a contract and, in certain circumstances, legal action.

39. The University may refer the user to the police where it reasonably believes a crime has been committed.

CoP Review

40. This CoP will be reviewed every two years. It is the responsibility of the Head of Cyber Security to ensure that these reviews take place and remains internally consistent.

41. Reviews resulting in minor changes shall be signed off by the Director of Digital Services prior to deployment. Substantial changes to the CoP shall be approved by the Digital Services Senior Management Board prior to deployment.

42. Substantive changes to this CoP shall be communicated to all relevant Users.

CoP Specifications

Organisation	Leeds Beckett University
Author(s)	Dominic Jennings (Cyber Security Assurance Analyst)
Developed in consultation with	Digital Services, Cyber Security, Information Governance, Registrar & Secretary's Office
Owner	Director of Digital Services
Target audience	All staff, students and all other relevant parties
Sensitivity	Public
EDI Assessment	The policy supports the principles of the university's approach to IT and Cyber Security and includes a commitment to complying with legal and regulatory requirements by adhering to applicable UK laws and regulations ensuring fair, transparent and equal implementation of controls. No significant EDI impacts have been identified. The CoP will continue to be monitored to ensure fairness, transparency, and equality of treatment for all users
Approved by	Director of Digital Services
Endorsed by	Digital Services Management Board
Effective from	11-04-2026
Last review date	11-04-2026
Next review date	+2 years from last date of approval [04-2028]
Status	**Published**
Distribution	All Services, Staff, Teams, and Users.
External references	None
Links to other internal policies / procedures	University policies | Leeds Beckett University
Version reference	1.0
Version History - summary of changes (inc. committee paper reference if applicable)	New CoP. Supersedes previous CoP/guidance contained in IT Security Policies.