Cryptography and Encryption Code of Practice

Executive Summary

The protection of sensitive information is paramount to maintaining the trust and integrity of the university's academic, administrative, and research activities. Cryptography and encryption are essential tools in safeguarding data against unauthorized access, ensuring that information remains confidential, intact, and available only to authorized individuals.

This CoP outlines the university's commitment to implementing robust cryptographic controls. By adhering to these internationally recognized frameworks, the university aims to mitigate risks associated with data breaches, cyber-attacks, and other security threats.

By implementing and enforcing this CoP the University aims to;

- ensure that the University complies with its legal and statutory obligations,
- protect the confidentiality, integrity and availability of information and systems, and,
- protects the interests of users of university systems and services

CoP Statement

1. The Cryptography CoP sets out when and how encryption should (or should not) be used. It includes protection of personal, confidential and commercially sensitive information and communications, key management, and procedures to ensure encrypted information can be recovered by the organisation if necessary.

Purpose

2. The purpose of this document is to define rules for the use of cryptographic and encryption controls, as well as the rules for the use of cryptographic keys, to protect the confidentiality, integrity, authenticity, and non-repudiation of information.

Scope and Application

3. This CoP applies to all university employees, students, third-party contractors and service providers, and any other individuals who have access to the University IT Environment. This includes users accessing from university premises or from remote locations and whether using university-owned or personal devices.

4. It encompasses all forms of data, including but not limited to, electronic communications, stored data, and data in transit.

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

6. 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.

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

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

Standards

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

10. 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

11. 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.

12. Cryptography - The practice and study of techniques for securing communication and data from unauthorized access or alteration.

13. Encryption - The process of converting information or data into a code, especially to prevent unauthorized access.

14. Data at Rest - Data that is stored on a device or server and is not actively being used or transmitted.

15. Data in Transit - Data that is actively moving from one location to another, such as across the internet or through a private network.

16. Encryption Algorithm - A mathematical procedure used to encrypt and decrypt data.

17. Encryption Key - A piece of information used by an encryption algorithm to transform plaintext into encrypted text and vice versa. Encryption keys are essential for the encryption and decryption processes, ensuring that data remains secure and accessible only to those with the correct key.

18. Key Management - The process of handling cryptographic keys, including their generation, storage, distribution, rotation, and destruction.

19. Multi-Factor Authentication (MFA) - A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.

20. Role-Based Access Control (RBAC) - A method of regulating access to computer or network resources based on the roles of individual users within an organization.

21. Hardware Security Module (HSM) - A physical device that provides extra security for managing digital keys and performing encryption and decryption functions.

22. TLS (Transport Layer Security) - A cryptographic protocol designed to provide secure communication over a computer network.

23. Secured Certificates - Digital certificates used to establish a secure connection between a client and a server. They are essential for ensuring the authenticity and integrity of the communication. Secured certificates are commonly used in protocols like HTTPS to encrypt data transmitted over the internet.

RESPONSIBILITIES

Responsibilities and application of the CoP

24. The Vice Chancellor is responsible for ensuring that all necessary resources are available to support the implementation of this CoP across the University.

25. The Director of Digital Services is responsible for the operational coordination of the CoP and 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)

26. This CoP forms part of a suite of related Information Security policies.

OPERATIONAL APPLICATION

Data Encryption

27. All sensitive university data (i.e. classified with a higher sensitivity than Public) stored on devices or servers must be encrypted using industry standard, strong encryption algorithms.

28. All sensitive data transmitted over networks must be encrypted using secure, non-deprecated protocols.

29. Encryption mechanisms should be kept in line with industry standards. If you are unsure, contact IT Services for further advice.

Remote network access

30. Access to cryptographic keys and encrypted data must be restricted based on roles and responsibilities (RBAC).

31. MFA must be used for accessing systems that handle cryptographic keys.

32. Facilities for encrypted connection to the University's IT systems and services via networks not fully within the control of the University's security management (e.g. the internet or wireless access), will be provided by IT Services and appropriate support given.

33. Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.

Managing Electronic Keys

34. Electronic cryptographic keys are used to encrypt and decrypt messages or digital signatures on messages sent between one or more parties. The management of these keys is critical if confidentiality, authenticity and integrity are to be preserved.

35. A procedure to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.

36. Cryptographic keys must be generated using approved methods and algorithms.

37. Keys must be stored securely, using hardware security modules (HSMs) or equivalent secure storage solutions.

38. Keys must be rotated regularly and upon suspicion of compromise.

39. Keys must be securely destroyed when no longer needed.

40. Keys need to be communicated by reliable and secure methods and kept confidential.

41. Key management procedures need to ensure that the source of the key is trustworthy.

Secured Certificates, Cryptographic Algorithms and Protocols

42. Approved cryptographic algorithms (e.g., AES, RSA, SHA-256) must be used during any encryption process.

43. Industry-standard protocols for encryption (e.g., TLS, IPsec) must be used during any encryption process.

44. Secured Certificates should be employed when embarking on any form of e-Commerce, online booking of distance learning, acceptance of electronic invoices, e-Procurement, or other process where reliance might be placed on the authenticity and integrity of information received.

45. Important business information being communicated electronically shall be authenticated using Secured Certificates. Information received without a Secured Certificate must not be relied upon.

46. When using Secured Certificates, consideration should be given to any relevant legislation that describes the conditions under which a digital signature is legally binding.

47. Unsupported ciphers, protocols and algorithms must be disabled where possible. Superseded or insecure protocols and cipher suites should not be used unless there is an approved exception in place.

48. Encryption algorithms and specific implementations of algorithms can contain vulnerabilities. The use of algorithms and encryption software must be monitored and managed through the vulnerability management process.

COP MANAGEMENT

CoP Review

49. 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.

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

51. 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.