IT and Cyber Security Policy

Executive Summary

Leeds Beckett University recognises that information is fundamental to its effective operation and considers it a critical business asset. The University is committed to the lawful and ethical use of information and to safeguarding the security of its information assets, along with the digital and physical infrastructure that supports them. This commitment underpins and enables the University's academic, research, administrative, and community engagement activities.

Policy Statement

1. The principles adopted by the University will align with its strategic goals and values, and are intended as an enabling mechanism for information sharing, electronic operations and for reducing IT and cyber security risks to acceptable levels. IT use must be lawful, ethical, and consistent with University policies.

Purpose

2. The purpose of this policy is to establish the principles and responsibilities for securing the University's assets, systems, and services.

3. It aims to ensure the confidentiality, integrity, and availability of information by protecting against cyber threats, ensuring compliance with legal and regulatory requirements, and promoting a culture of security awareness.

Scope and Application

4. All information assets owned, processed, or managed by the University, regardless of format or location, including those stored, accessed, or transferred overseas. Where information is held or processed outside the United Kingdom, appropriate legal, technical, and organisational safeguards must be applied.

5. All systems and services used to store, transmit, or process University data.

6. All staff, students, contractors, and third parties who access or manage University information systems.

7. The policy applies throughout the lifecycle of information assets, from creation, through storage and utilisation, to disposal.

8. Information security is defined as the preservation of:
   - Confidentiality (protecting information from unauthorised access and disclosure)

- Integrity (safeguarding the accuracy and completeness of information)
- Availability (ensuring that information and associated services are available to authorised users when required)

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 Policy.

10. The Policy also supports adherence to the requirements contained within various acts of parliament and other legislation and relevant certification schemes, including, but not limited to;

    Computer Misuse Act
    Data Protection Act
    Freedom of Information Act
    Copyright, Designs and Patents Act
    Regulation of Investigatory Powers Act
    Human Rights Act
    Electronic Communications Act
    Digital Economy Act
    Obscene Publications Act
    Counterterrorism and Security Act
    Cyber Essentials

Definitions

11. Assets – Any valuable resource that needs protection from compromise or potential attack. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., data, information, software, system, cloud-based platforms, patent, or intellectual property). The value of an asset is determined by the potential impact on the University in terms of operational, informational, reputational, legal, or financial risk should the asset be lost, compromised, or rendered unavailable.

12. Security Breach - Is any incident or activity that causes, or may cause, a break down in the availability, confidentiality, or integrity of the physical or electronic information assets of Leeds Beckett University.

13. User – any person directly or indirectly accessing the University IT Environment.

14. Student - Any individual enrolled on a Leeds Beckett University programme of study, including apprentices registered on University's degree apprenticeship programmes and those at partner institutions registered as LBU students.

15. Staff - Any individual on a contract of employment including officers, employees (whether permanent, fixed term or temporary), workers, trainees, seconded staff, agency staff, volunteers, interns or any other person working in any context within the University.

16. Associated person or body - Any person or body engaged on University business by which we mean individuals performing or providing services for or on behalf of the University. This may include governors, University subsidiaries, contractors, recipients of grants, partners, collaborative arrangements, joint ventures, agents and advisors etc. For the purposes of the Policy, this also includes any third parties representing the University.

RESPONSIBILITIES

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

18. The University Executive Committee is accountable for approving and supporting this policy.

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

20. The Head of Cyber Security is responsible for developing and maintaining the University's cyber security programme, coordinating risk assessments and incident response, and reporting on security posture to senior leadership.

21. Digital Services is responsible for implementing technical controls, monitoring systems, supporting secure infrastructure, and enabling disaster recovery.

22. Hardware and software purchases will go through the institutionally approved procurement processes, but will additionally be subject to the approval of the Director of Digital Services (or nominee).

23. The Information Governance Manager is responsible for implementing non-cyber security related information protections, such as records management and compliance with information law.

24. The University Registrar and Secretary has ultimate responsibility for business continuity.

25. Data Owners are responsible for ensuring appropriate classification and protection of data under their control.

26. All Users are responsible for complying with this policy, and relevant Codes of Practices and procedures protecting university assets, reporting suspected security incidents or breaches, and completing mandatory security awareness training.

Consequences and Sanctions

27. The University may suspend or withdraw systems access to users who breach this policy without notice to them and take further action as appropriate.

28. Breaches of this policy by University staff or students may result in disciplinary procedures, up to and including dismissal.

29. Contractors and associates may also face sanctions such as termination of contracts or reporting to professional regulators.

30. The University reserves the right to report criminal offences to the appropriate authorities and pursue legal remedies.

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

31. This top-level policy is part of a suite of related information and cyber security documents.

32. The principles in this policy, and their practical application, are further defined and supported by the following codes of practice.

Document Name
Supplier Security Code of Practice
Acceptable Use Code of Practice
Access Control Code of Practice
Cryptography and Encryption Code of Practice
Asset Management Code of Practice
Secure Development Code of Practice
Patch Management Code of Practice
Mobile Device and Remote Working Code of Practice
Physical and Environmental Security Code of Practice
Logging and Monitoring Code of Practice
Bring Your Own Device (BYOD) Code of Practice
Anti-Malware Code of Practice
Information Transfer Code of Practice
Network Management Code of Practice
AI Cyber Risk Awareness Code of Practice

OPERATIONAL APPLICATION

IT and Cyber Security Principles

The University will:

33. Protect its information assets by assessing risk and implementing appropriate technical, physical, and administrative controls to protect information assets from unauthorised access, disclosure, alteration, or destruction.

34. Comply with legal and regulatory requirements by adhering to applicable UK laws and regulations (including the Data Protection Act 2018, the General Data Protection Regulation) and sector-specific guidance (such as those from Jisc and UCISA), and ensure that use of university information and infrastructure is lawful, ethical, and consistent with university policies.

35. Promote a culture of security awareness by providing regular training and awareness to ensure all users understand their responsibilities and the importance of cyber security.

36. Respond to security incidents by maintaining a robust incident response capability to detect, report, and recover from information security breaches in a timely and effective manner.

37. Continually improve the University's cyber security posture by regularly reviewing and updating security policies, procedures, and controls to adapt to emerging threats and changes in the technological and regulatory landscape.

POLICY MANAGEMENT

Policy Review

38. This policy will be reviewed every three years, or in response to significant changes in legislation, technology, or risk landscape. It is the responsibility of the Director Digital Services to ensure that these reviews take place and remain internally consistent.

39. Reviews resulting in minor changes shall be signed off by the Director of Digital Services prior to deployment. Substantial changes to the policy shall be approved by the University Executive Committee prior to deployment.

Training, Awareness, and Compliance Reporting

40. Digital Services will ensure that this policy is effectively communicated and embedded across all areas of activity through appropriate training, awareness initiatives, and integration into local procedures and risk management records.

41. Assurance on implementation and compliance will be provided to the University Executive Committee and/or the Audit & Risk Committee as required. Internal Audit will provide independent assurance on the adequacy and effectiveness of the University's cyber security controls, routinely reporting findings to the Audit & Risk Committee.

42. Compliance with mandatory training requirements will be monitored and reported to the Audit & Risk Committee.

Document Control

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 outlines the principles of the university's approach to IT and Cyber Security, which include a commitment to comply 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 policy will continue to be monitored to ensure fairness, transparency, and equality of treatment for all users.
Approved by	University Executive Committee
Endorsed by	Digital Services Management Board
Effective from	18-02-2026
Last review date	18-02-2026
Next review date	+3 years from last date of approval [02-2029]
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 Policy. Supersedes previous policy/guidance contained in IT Security Policies.