Physical and Environmental Security Code of Practice

Executive Summary

This CoP outlines the principles for preserving the security of Leeds Beckett University IT Environment from threats originating from its physical location.

This CoP sets out the approach to be adopted to manage, develop, improve, and assure Physical Security across the University.

It is essential that the University environment is secure and where potential threats (including those from both natural and human-made hazards, terrorism, crime, and insider threats) to the University IT Environment have been identified, risk assessed and appropriately mitigated to prevent interference, loss, or compromise (malicious or otherwise).

This includes ensuring physical and environmental perimeters are protected and entry controls are in place to provide proportionate protection against possible threats, such as natural disasters and terrorist attacks.

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, and
- provide authorised users of university IT with a safe and acceptable working environment.

CoP Statement

1. The security and preservation of the University IT Environment is of paramount importance. The University possesses and uses computer systems, networks, hardware, software, and data as an integral and pervasive part of its operations.

2. Physical and environmental security refers to measures that are designed to protect physical locations and the assets, information and personnel contained within. Physical and Environmental Security controls must be implemented that are proportionate to the risk appetite of the University.

Purpose

3. The purpose of this CoP is to ensure the protection of the university's information and information processing facilities from unauthorized physical access, damage, and interference.

4. It is intended to protect premises, property, staff, students, contractors, and visitors from physical security threats that could reasonably be foreseen.

5. 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

6. This CoP applies to all university-owned or operated facilities, including data centers, offices, and any other locations where information processing activities occur.

7. All staff and Students, contractors and visitors must ensure they remain observant, report suspicious behaviour to estates, and highlight non-compliance. This vigilance will help deter, delay, prevent and/or detect unauthorised access to, or attack on, a location and mitigate the impact should they occur.

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

9. 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.

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

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

Standards

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

13. 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

14. 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.

15. 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, patent, or intellectual property)

16. User – any individual afforded access to the University IT Environment via a direct relationship with the university, including Students, Staff and Associated persons or body's

17. 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.

18. 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.

19. 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 which may include governors, University subsidiaries, contractors, recipients of grants, partners, collaborative arrangements, joint ventures, agents and advisors etc. For the purposes of the CoP, this also includes any third parties representing Leeds Beckett.

20. Clear Desk and Clear Screen Practices - practices related to ensuring that sensitive information, in both digital and physical formats, and assets are not left unprotected at personal and public workspaces when they are not in use, or when someone leaves their workstation, either for a short time or at the end of the day.

RESPONSIBILITIES

Responsibilities and application of the CoP

21. 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.

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

23. 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)

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

OPERATIONAL APPLICATION

Physical Security

25. All equipment that provides access to University information should be kept secure by physical means or by using good practice. This should be achieved by establishing secure perimeters around areas containing sensitive or critical information and information processing facilities, and implementing physical barriers such as fences, walls, and controlled entry points to prevent unauthorized access

26. Clear desk and clear screen practices must be implemented.

27. File servers and equipment that store or process information classed as Confidential or Internal - All Staff must be in physically secured areas.

28. Entry to secured areas shall be restricted to authorised users.

29. Staff, students or contractors must not lend their entry card to anyone or allow anyone to follow them through card-controlled doors (tail-gating).

30. Physical access rights must be revoked immediately for staff who leave the employment of the University.

31. Other visitors must only be granted access to secure areas for specific and authorised purposes only and must be supervised.

32. A log must be maintained of all access to restricted or secure areas and these logs regularly reviewed.

Cabling

33. Cables between buildings should be underground wherever possible.

34. Ducts and entry points into buildings should be secure and inspected annually for signs of damage or interference. A log of these inspections shall be retained by the Estates team.

35. Internal cabling should be used wherever possible, and cabling within buildings should be installed in ceiling voids and secure ducts.

Wireless Access Points

36. Wherever possible, wireless access points should be installed at a high level to make them less exposed and more secure from theft or tampering.

Communications racks and wiring cabinets

37. All communications equipment must be kept secure, either in locked rooms or in racks and cabinets with locks.

38. Keys to communications rooms, racks and cabinets shall be held securely so that they are not available to individuals who are unauthorised to access network devices.

Environmental controls

39. Risks from natural disasters (e.g., floods, fires) and man-made threats (e.g., vandalism, theft) must be assessed and appropriate mitigations implemented.

40. Appropriate environmental controls, such as fire suppression systems, temperature and humidity controls, and uninterruptible power supplies (UPS), must be installed and maintained.

41. Regular risk assessments and must be conducted and any mitigation strategies updated as necessary.

42. Data centres must be protected by appropriate air conditioning and very early smoke detection systems.

43. Temperatures in data centres must be monitored and undue variances reported immediately to the Estates and Digital Services department.

44. Equipment must be protected from power failures or electrical anomalies.

45. Data centres must be protected by suitable local stand-by power supplies, either a generator or uninterruptible power supply.

46. Wiring cabinets, and the rooms in which they are located, should be inspected annually to assess security risks and hazards arising from environmental conditions.

47. A log of these inspections shall be retained.

Equipment Maintenance

48. Equipment shall be maintained in accordance with manufacturers' recommendations to ensure its availability and integrity.

49. A log of all regular maintenance checks such as PAT testing must be recorded.

50. An inventory must be maintained of file servers and communications equipment and recorded in the current Asset Management System, which must be regularly checked to ensure that the University's information assets are accounted for.

Disposal of Equipment

51. All items of user equipment containing storage media must be returned to the Service Desk and shall have any software or sensitive data irretrievably removed before disposal.

52. All servers and network equipment must be decommissioned and disposed of in line with the data classification CoP.

53. Disposal of electrical and electronic equipment must be processed in accordance with WEEE regulations, by a company that is accredited by ICER (Industry Council for Electronic Equipment Recycling) to recycle IT equipment and that will provide certification of destruction.

COP MANAGEMENT

CoP Review

54. 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.

55. 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.

56. 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.