Acceptable Use Code of Practice

Executive Summary

This Code of Practice (CoP) outlines principles for the acceptable use of the Leeds Beckett University (the University) IT Environment.

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. This CoP outlines principles for the acceptable use of the University IT Environment, what is considered unacceptable use, and what responsibilities users have in ensuring that it is used in an acceptable manner.

Purpose

3. The purpose of this CoP is to outline the acceptable use of resources that constitute the IT infrastructure of the University.

4. It is intended to ensure that the University's IT Environment is used appropriately and lawfully by its Users. Failure to do so could result in operational and reputational damage to the University.

Scope and Application

5. This CoP applies to all University employees, associates, consultants, contractors, casual workers, agency workers, students, volunteers and interns who may use University IT systems.

6. It also applies to anyone else who has access to University IT systems directly or indirectly. This CoP does not form part of any employee's contract of employment and the University may amend it at any time at its sole discretion.

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

8. Breaches of this CoP by University staff may result in disciplinary procedures including dismissal.

9. The University may suspend access to users who breach this CoP without notice to them and take further action as appropriate.

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 – 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)

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

15. 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.

16. 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.

17. 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 CoP, this also includes any third parties representing the University.

RESPONSIBILITIES

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

19. 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)

20. This CoP forms part of a suite of related information security policies.

21. The JANET Acceptable Use Policy applies to all users of the University IT systems and services.

OPERATIONAL APPLICATION

Acceptable use

22. Users shall use the University IT Environment in a responsible manner that respects the rights and privacy of others, avoiding activities that could harm or disrupt other users, or disrupt other users of University or third-party IT system.

23. Users shall comply with all applicable laws and regulations, and university policies when using the University IT Environment.

24. The University IT Environment is provided primarily for university business purposes to support teaching, learning, research and enterprise, and professional and administrative activities.

25. Authorised users are allowed to make reasonable personal use of the University IT Environment provided this does not; interfere with its security; interfere with the performance of their duties; cause financial loss to the university; or cause difficulty or distress to others.

26. Users must obtain explicit permission from the appropriate Resource Centre Manager and Digital Services to use the University IT Environment for personal commercial gain, and this may be subject to a charge.

User Responsibilities

Responsibility for assets

27. Each asset comprising the University IT Environment will have an assigned owner. The asset owner is responsible for the confidentiality, integrity, and availability of the asset in question.

28. Assets may not be used in ways that contravene the requirements of University policies and procedures.

29. Users must return all University assets to an appropriate manager, or divest of access to applicable University assets, upon the expiration or termination of their formal or informal engagement with the University.

Backup

30. All University information shall be backed up appropriately according to its sensitivity and the requirements of any applicable records retention schedules.

31. Asset owners, with assistance from Digital Services, are responsible for ensuring that backup arrangements published or agreed with users of the system are reliably implemented and that users are informed promptly should there be any problems with or changes to the backup arrangements.

32. Users shall store digital University information in approved storage locations that have established, automated backup processes.

Access to the IT Environment

33. Users of the University IT Environment shall only attempt to use or access assets for which they have appropriate authorisation.

34. Users must not take part in activities that intentionally or inadvertently bypass controls designed to control or restrict access.

35. Users shall only use assets for authorised purposes.

Account and Password responsibilities

36. Where a user has been issued with a user ID and password, the user is responsible for all activity attributable to that identity.

37. Users shall take all reasonable steps to prevent their User identity from being used by anyone else.

38. Administrative account holders must take all reasonable steps to prevent the administrative identity from being used by anyone else.

39. Users must enable Multi-Factor Authentication on their network account in line with University requirements.

40. If a user suspects that their password is no longer secret, they must change their password at the first opportunity and report this to the Service Desk.

41. Users shall ensure that University allocated devices (such as a laptop or desktop) are restarted or shutdown at the end of the working day.

42. Users shall not allow another person to use their account and shall not use an account allocated to any other user.

43. The use of generic accounts or usernames shall be avoided unless there is an approved business reason that has been appropriately risk assessed.

44. Users shall follow University security procedures and guidance when selecting and using passwords.

45. Users must keep account passwords private and must not share them with anyone else.

46. Users shall protect the security of their passwords by avoiding their recording (e.g. writing down or stored in an automated log-on system such as a macro or browser) unless using a secure, university approved depository such as a password manager.

47. Users shall also exercise caution when entering passwords into log-in screens such that the likelihood of credential theft via phishing is minimised.

48. Users shall change default passwords at first log-on to any system where this is not automatically enforced.

49. Users shall ensure that passwords for accounts that allow access to the University IT Environment are entirely unique, both from previous passwords and from passwords protecting other accounts.

Protecting Against Unknown or Malicious Code

50. Users shall treat files communicated electronically, such as those downloaded from the internet or received via email, with the utmost care such that the likelihood of a successful cyber-attack is minimised. This includes assessing the validity of a file and the veracity of its source before being opened.

51. Users shall report suspected instances of malicious files, code or communications via appropriate reporting channels and inform both the IT Service Desk and Cyber Security team.

52. University approved anti-virus must be installed on all University IT Environment assets, which shall be kept fully up to date and used to scan all files prior to opening or launching.

53. This AV must not be tampered with unless explicit authorisation has been granted by Digital Services.

Clear desk and screen CoP

54. When away from their workspace users shall ensure that any physical media containing information classed as 'Internal – All Staff' or 'Confidential' is secured in such a way as to prevent unauthorised access.

55. Users shall always be mindful of the risk of unauthorised access to digital information viewed on device screens over which they have control.

56. Lock-screen and other applicable precautions designed to remove information from visibility when away from a workspace, such as logging out of systems or switching off devices, shall be taken where there is a risk of unauthorised access occurring.

Internet use

57. Internet may be accessed only through the University's local network with appropriate infrastructure and firewall protection. Direct Internet access through modems, mobile internet, wireless network, or other devices for direct Internet access is forbidden.

58. Access to some Internet pages for individual users, groups of users or all employees at the University may be blocked to protect users and the university from harmful or illegal content. Users must not try to bypass such restriction autonomously.

59. The user must regard information received through unverified websites as unreliable. Such information may be used for business purposes only after its authenticity and correctness have been verified.

60. Users are responsible for all possible consequences arising from unauthorised or inappropriate use of Internet services or content.

61. Admin accounts must not be used for standard use e.g. general internet browsing, email management.

E-mail and other message exchange methods

62. Users must only use University approved message exchange methods to communicate University data.

63. Users must not send communications containing information that is false, misleading, malicious, inaccurate, or impersonating another entity.

64. It is forbidden to send communications that are illegal as defined under law.

65. Users must not send spam messages to persons with whom no business relationship has been established, to persons who did not consent to receiving such information e.g. under the terms of an applicable privacy notice.

66. Users must save messages containing data significant for the University's business in accordance with University Records Management policies.

67. Each externally sent e-mail message must contain this disclaimer.

68. Users must avoid the creation of email forwarding rules from university accounts to other accounts.

Copyright

69. Users must not make unauthorised copies of software available in the University IT Environment.

70. Users must not copy software or other original materials from other sources and are liable for all consequences that could arise under intellectual property law.

71. Users must not install software on university devices that is not licensed by the university.

Incidents

72. Users of the University IT Environment shall report any security weakness, incident, event or breach to the IT Service Desk and Cyber Security team as soon as they become aware of it.

Unacceptable Use

73. Users shall not engage in any form of unlawful activity within the University IT Environment as set out below.

74. Users shall not act in a way that bypasses information security safeguards, including tampering with devices, or contradicts or undermines either the preceding CoP statements or other University policies.

75. The creation, display, download, production, store, circulation or transmission of unlawful material, or material that contravenes university policies or codes of conduct. The University reserves the right to block or monitor access to such material.

76. Users must not continue to use University IT Environment assets after the Director of Digital Services has requested that usage to cease due to causing disruption to the correct functioning of University systems.

77. Users must avoid either attempting or facilitating unauthorised access to the University IT Environment, either through direct actions or by facilitating such access.

78. Users must not use “open access” computing facilities (such as computer labs or library computers) for recreational or other non-University work when there are others waiting to use the resource.

79. Users must not in any way cause any form of damage to the University IT systems and services or the associated hardware.

80. Users must not use information assets in a manner that unnecessarily takes up capacity, weakens the performance of or poses a security threat to the University IT Environment.

81. Users must not attempt to install or use software or applications, or download and run program code from external sources, on devices unless it has been formally authorized via the appropriate university approval process.

82. Users must not install personally licensed software on university devices.

83. Users must avoid running software or opening files obtained from untrusted sources and be particularly cautious of accessing files attached to unsolicited email and stored on untrusted media.

84. Users must not use non-university cryptographic tools (encryption) on devices, unless specific exemptions are referenced in other university policies. This is to prevent files from being inaccessible by monitoring.

85. Users must not install or use peripheral devices such as modems, memory cards, external hard drives or other devices for storing and reading data (e.g. USB flash drives) unless it has been risk assessed and approved by Digital Services management prior to its use.

86. Users must not attempt to gain access to restricted areas of the network or areas that are not necessary for the performance of their duties or attempt to gain access to any password-protected information unless authorised to do so in the proper performance of their duties.

87. Users must not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

Monitoring the use of information and communication systems

88. The University's systems enable it to monitor email, internet and other communications. For the University's operational reasons, and to carry out legal obligations in its role as an employer, the use of University systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for the University's business purposes.

89. The University reserves the right, without notice to Users, to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) and any use of its IT systems as reasonably necessary including but not limited to the following purposes:
    (a) To monitor whether use of the email system or the internet is legitimate and in accordance with this CoP.
    (b) To find lost messages or to retrieve messages lost due to systems failure.
    (c) To assist in the investigation of alleged wrongdoing.
    (d) To comply with any of its legal obligations.

90. The University may use specialised tools for the purpose of identifying and blocking forbidden methods of communication and filtering forbidden content.

COP MANAGEMENT

CoP Review

91. 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 remain internally consistent.

92. 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.

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.