Bring Your Own Device (BYOD) Code of Practice

Executive Summary

In some circumstances Leeds Beckett University permits the use of devices not owned by the university for work-related activities. This includes devices such as those personally owned by staff members and is commonly known as 'bring your own device' or BYOD.

Such use must comply with this Code of Practice (CoP) to;

- ensure that the security of the University IT Environment is maintained.
- ensure that the University complies with its legal and statutory obligations.
- protect the interests of users of the University IT Environment.

CoP Statement

1. Leeds Beckett University supplies IT equipment to University users for the conducting of University business. However, there are some situations where the use of non-university owned devices, or BYOD, is permitted.

2. The use of BYOD creates issues that need to be addressed, particularly around cyber and information security. For example, the University must remain in control of data for which it is responsible regardless of the ownership of the device used to carry out the processing

3. It is essential that non-university owned devices are secured in accordance with professional best practice and with statutory, regulatory, and contractual requirements around cyber security.

Purpose

4. The purpose of this CoP is to define how Leeds Beckett University will retain control of and continue to protect its University IT Environment when information is processed by, or systems and services are accessed through, IT devices that are not owned and configured by the University.

Scope and Application

5. This CoP applies to all employees, contractors, academics, students, and any other individuals who use non-university owned devices to access the University IT Environment.

6. This CoP applies to all BYOD that can store, transfer, or process information, or that can access systems or services, regardless of from where that access occurs i.e. both on-site and remote/external access.

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

8. 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.

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

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

Standards

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

12. 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

13. BYOD – Bring Your Own Device. Refers to any IT device that is not owned, procured or configured by the University.

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. Asset - 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. IT Devices – This includes laptops, smart phones, tablets, USB memory sticks, digital cameras, and any other similar electronic devices.

21. 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.

22. PIN – Personal Identification Number

23. MFA – Multi-Factor Authentication. This is where a form of authentication is required in addition to username and password before access is granted. This could be a prompt sent via an authenticator app installed on your phone or a one-time code that must be inputted into an authenticator app.

RESPONSIBILITIES

Responsibilities and application of the CoP

24. 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.

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

26. 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.

27. BYOD owners are responsible for ensuring that the requirements of this CoP are enforced when using relevant devices.

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

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

OPERATIONAL APPLICATION

Device Eligibility

29. Only BYOD that meet the university's security requirements are permitted to access university systems and data.

30. BYOD must support the universities security control requirements.

31. Where it is contractually required, Digital Services will maintain a list of approved BYOD and operating systems.

32. Users must provide device details, including make, model, and operating system version. Digital Services will verify that the device meets the necessary security requirements stipulated in applicable third party contracts.

33. Users must notify Digital Services when applicable BYOD is being disposed of, sold, or handed to a third party for servicing to ensure any list of approved BYOD is kept up to date and university data is removed.

Security Requirements

34. BYOD users must ensure that the device operating system, firmware and installed software is patched and up to date. Critical security patches must be applied within 14 days of release.

35. BYOD must be protected by a physical or software firewall.

36. BYOD used to access University IT systems and services and that are at risk of malware infection must run AV (anti-virus) software that is continuously updated.

37. AV software must be configured to perform real-time scanning and periodic full system scans, including scans for potentially malicious websites and warnings against accessing them.

38. Some University IT Systems and Services can remotely delete data and in certain circumstances this may be actioned to prevent unauthorised access to the University IT Environment. Users should be aware that in the event of this happening it may also impact the user's personal data.

39. Should the university introduce 'Mobile Device Management' software that enables remote wipe functionality, BYOD must support this software and users must adopt it to continue using University services on BYOD.

40. Auto-run or auto-play functionality on BYOD must be turned off to avoid the unintended installation or triggering of malicious software.

Access Control

41. All BYOD devices must require authentication via password or PIN to access. These must meet any complexity requirements set out by the University.

42. BYOD accessing the University IT Environment will be automatically forced to create a password or PIN where it is technically possible to do if these are not already in place.

43. Default passwords for admin and/or users accounts on BYOD must be changed to meet the any complexity requirements set out by the University.

44. BYOD users must prevent anyone else from accessing the device being used to access the University IT Environment.

45. Access to the University IT Environment through BYOD must otherwise be managed in line with the Access Control CoP (link).

Data Protection

46. Users must not synchronise BYOD with cloud storage or services such that university data classified as personal, confidential, or commercially sensitive is stored locally on BYOD.

47. Users must only access data classified as personal, confidential, or commercially sensitive on BYOD that is solely used by that individual user.

48. If it is unavoidable, University data stored on BYOD must be encrypted both in transit and at rest. This includes using industry standard, secure communication protocols and device encryption.

49. Remote access to university systems must be via a secure Virtual Private Network (VPN).

50. Individuals using BYOD must seek guidance from Digital Services if they are unsure about the back-up arrangements for any university data.

User Responsibilities

51. If a domestic wireless solution is used at the user's premises, it must be made secure utilising the wireless security features and password included with the wireless solution, to ensure no unauthorised access is permitted.

52. BYOD users must not attempt to bypass or remove device restrictions and security controls imposed either by the manufacturer or by the university. This includes any attempt to "root" or "jailbreak" devices to allow the installation of unapproved or unauthorised software, firmware, or unsigned applications, or to gain access to functionality not intended to be exposed to the user.

53. The use of software applications on BYOD for processing university data must be appropriately licensed e.g. business use license.

54. The physical security of BYOD must be maintained when used outside of University premises. BYOD must not be left unattended in unsecured areas.

55. BYOD users must ensure that confidential data accessed using the device cannot be read by unauthorised persons, particularly when in public spaces.

56. Any potential data breach, loss or compromise of commercially sensitive data, or suspected cyber incident involving BYOD, should be reported via the established incident reporting process.

Monitoring and Auditing

57. The university reserves the right to monitor the use of BYOD to ensure compliance with this CoP.

58. Monitoring may include reviewing access logs, conducting security assessments, and auditing device configurations. Users will be notified of any monitoring activities.

59. Where contractually required, regular audits will be conducted of BYOD to ensure compliance with this CoP and identify any security risks.

60. Audits may include reviewing device registrations, access logs, and security configurations. Any non-compliance issues will be addressed promptly.

Termination of Access

61. The university reserves the right to revoke access to university systems and data from personal devices at any time.

62. Access may be revoked for non-compliance with this CoP, security concerns, or changes in user roles. Users will be notified of any access revocations.

63. Upon termination of access, users must remove all university data from their personal devices.

64. If applicable, Digital Services will assist users in securely removing university data from their devices. Users must confirm that all data has been removed.

65. The University reserves the right to withdraw support of BYOD

COP MANAGEMENT

CoP Review

66. 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.

67. 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.

68. 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.