# Asset Management Code of Practice

## Executive Summary

This Code of Practice (CoP) enables the University to ensure that all IT asset will be managed effectively and securely, and asset users understand their responsibility in the effective management of University IT assets.

By following this CoP, the University can;

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

**CoP Statement**

1. The University has made significant investment in IT assets to facilitate its operations. A CoP for managing those assets is vital in providing assurance that this will be done effectively through the lifecycle of those assets.

**Purpose**

2. The purpose of this CoP is to establish a comprehensive framework for managing the university's IT assets, including information and physical assets.

**Scope and Application**

3. This CoP applies to all University IT assets and users of them.

4. This CoP will be provided to all new and existing staff and members of the University who have a responsibility for the use and management of assets.

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. 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)

13. 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

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 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.

**RESPONSIBILITIES**

**Responsibilities and application of the CoP**

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

18. 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)**

19. This CoP forms part of a suite of related Information Security policies that can be found here (insert link).

**OPERATIONAL APPLICATION**

20. An up-to-date inventory of all IT assets must be maintained, including their classification based on sensitivity, value, and criticality where appropriate.

21. Information about physical IT assets will be held in an asset management system, which will be maintained by Digital Services, to enable the assets to be tracked, managed and audited throughout their lifecycle.

22. IT assets will be administered and maintained to ensure they remain fit for purpose and compliant with the licenced conditions of use during their lifecycle.

23. All IT assets purchased by the University are the property of university and will be deployed and utilised in a way that is deemed most effective for addressing the University's needs and objectively demonstrates value for money.

24. All physical IT assets purchased by the University will be stored in centralised asset management stores managed by Digital Services when they have not been issued or are not in use.

25. Requests for physical IT assets must be submitted via the Service Desk in accordance with current ordering processes and procedures.

26. Digital Services will assess requests for new and replacement IT equipment and fulfil them with standard equipment that best fits the requirement, and by aiming to reissue assets held in the centralised store in the first instance.

27. The procurement of IT assets must be undertaken in consultation with and carried out by Digital Services from inception.

28. Digital Services is responsible for engaging with the University's Procurement Team and ensuring that the best procurement practice is followed as per the University's policies and applicable legislation.

29. On behalf of the University and in consultation with the Procurement Team, Digital Services is responsible for identifying and managing sources and channels for the purchase of IT assets, utilising existing framework agreements whenever possible.

30. All IT assets (excluding consumable items, e.g. keyboards, mice, etc.) will be registered in the asset management system and be asset tagged before being issued or put into use.

31. Ownership of information assets must be assigned to designated individuals or departments responsible for their management and protection.

32. Individual users or departments will be held responsible for protecting the IT assets that have been assigned to them against physical or financial loss whether by theft, mishandling or accidental damage, by using appropriate physical security measures.

33. Access to information assets must be restricted to authorized personnel only, based on the principle of least privilege.

34. Appropriate security measures must be implemented to protect information assets from unauthorized access, disclosure, alteration, and destruction.

35. Users must not install unapproved software on to IT assets. Requests should be made to the Service Desk to have additional software installed on to a device.

36. Any software installed must be legitimately purchased and licensed for its purpose of use by the university.

37. Accurate records of asset acquisition, usage, maintenance, and disposal must be maintained.

38. Users or designated owners must contact the Service Desk if they need to move, reassign or return IT equipment.

39. IT assets that are no longer in use, such as when an employee leaves, must be returned to the University via the Service Desk.

40. To ensure the confidentiality of information, any IT asset that has been used to process or store personal or sensitive information must be reimaged before reissue and must go through a physical disposal and destruction process at the end of its useful life.

41. If an asset is lost or stolen, it should be reported to the Service Desk as soon as possible and the associated asset record updated.

42. If an asset becomes faulty or broken and cannot be repaired by a University approved supplier, a replacement device should be issued. Associated asset records updated must be updated accordingly.

43. The Service Desk will dispose of assets in line with the University's WEEE recycling contractor. All destruction certificates are stored within the IT department.

44. Regular audits and reviews of information assets should be performed to ensure compliance with security policies and identify areas for improvement.

45. Breach of this CoP may result in relevant assets being remotely wiped, blocked from the University's network, and/or being prevented from using University provided services and software.

## COP MANAGEMENT

### CoP Review

46. 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.

47. 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.

48. 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. |