Anti-Malware Code of Practice

Executive Summary

The primary objective of this anti-malware CoP is to safeguard the University's information systems and data from malicious software threats. It aims to protect the University's IT Environment from malware threats by establishing guidelines for the prevention and detection of, and response, to malware incidents.

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. Malware, which includes viruses, worms, ransomware, and spyware, poses significant risks to the security and functionality of IT systems. These threats can lead to data breaches, financial losses, operational disruptions, and damage to the organization's reputation.

2. By implementing robust anti-malware measures, the organization seeks to protect its digital assets, ensure the integrity and confidentiality of sensitive information, and maintain the overall security of its IT Environment.

3. Additionally, this CoP outlines the responsibilities of employees and IT personnel in adhering to best practices for malware prevention and response, thereby fostering a culture of cybersecurity awareness and vigilance across the organization.

Purpose

4. The purpose of this CoP is to establish a framework for the detection, prevention, and mitigation of malware attacks.

5. It is intended to protect individual users, the university, and its partners from the impact of malware incidents. Without this 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 employees, third-party contractors and service providers, and any other individuals who access the University IT Environment.

7. It covers the entirety of the University IT Environment, including personal BYOD that connect to the university's network or access its data.

8. Unless explicitly stated otherwise in this CoP, the JANET Acceptable Use Policy applies to all users of the University IT systems and services.

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

10. This CoP will be provided to all new and existing staff, students, and members of the University.

11. All other users of the University's information systems shall be advised of the existence of this CoP, which shall be made available to them.

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

13. 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.

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

15. The University may refer the user to the police where it reasonably believes a crime has been committed.

Standards

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

17. 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

18. 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.

19. 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)

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

21. 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.

22. 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.

23. 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.

24. Malware - a piece of computer code, most often a malicious software program designed to destroy or damage information on computers. Some viruses cause no damage apart from reproducing, but a significant number are specifically designed to cause data loss or to compromise the confidentiality of files by sending copies of them to others.

    Potential sources of viruses include external storage media such as USB sticks or hard-drive, e-mail attachments, software or digital documents copied over networks, and malicious links, files or website traffic transferred over the Internet.

RESPONSIBILITIES

25. 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.

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

27. 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)

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

OPERATIONAL APPLICATION

Anti-Malware Measures

29. All devices comprising the University IT Environment commonly affected by malware must have approved anti-malware software installed.

30. Anti-malware software must be regularly updated to ensure the latest virus definitions and security patches are applied. Automatic updates should be enabled wherever possible.

31. Anti-malware software should be configured to perform regular scans of the entire device system, including real-time scanning of files as they are accessed or downloaded, including on-access scans when external storage devices such as USB drives are connected.

Email and Web Protection

32. Email filtering solutions must be implemented to scan incoming and outgoing emails for malware, phishing attempts, and other malicious content.

33. Web filtering tools must be in place to block access to known malicious websites and prevent the download of harmful files.

Regular System Scans

34. Full system scans should be conducted at least once a week on all devices. Quick scans should be performed daily.

35. Scans should cover all files, directories, and external storage devices connected to the system.

36. Any detected threats must be reported immediately to the IT department for further analysis and action.

37. Detected malware should be quarantined or removed promptly to prevent further spread and damage.

Patch Management

38. All operating systems, applications, and firmware must be kept up to date with the latest security patches.

39. Where possible, automated patching should be enabled to minimise the window of potential exploitation.

40. Systems should be regularly assessed for vulnerabilities and patches applied promptly to mitigate risks.

41. Patches should be tested in a controlled environment before deployment to ensure they do not disrupt existing systems and applications.

User Training and Awareness

42. The university must ensure that the importance of anti-malware measures and best practices for avoiding malware infections are regularly communicated to users. This should be facilitated by the following activities;

43. Ongoing awareness campaigns will be implemented to ensure that cybersecurity top of mind for all staff members;

44. Periodically running of phishing simulations to test and improve employees' ability to recognise and respond to phishing attempts;

45. Provide accessible resources and guidelines for employees to reference regarding safe cyber practices and malware prevention.

Incident Response

46. Procedures for the detection, containment and eradication of malware, including isolation of infected systems, must be established. These should be automated where possible and appropriate.

47. A procedure for manual user reporting of suspicious malware related activity must be established.

48. A process for recovering from a malware incident, including restoring systems from backups and documenting the incident for future reference, must be established. This should include post-incident root cause analysis, incident evaluation and lessons learned.

Network Security

49. Network controls designed to prevent the occurrence of malware incidents should be implemented and maintained. These include; firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules; deployment of IDS/IPS solutions to detect and prevent potential threats and unauthorized access to the

network, network segmentation to isolate critical systems and data, reducing the risk of widespread malware infections; and enforcement of strong access controls and authentication mechanisms to ensure only authorized personnel can access sensitive systems and data.

Software and File Integrity

50. File integrity monitoring (FIM) solutions to detect unauthorized changes to critical system files and configurations should be implemented.

51. Digital signatures should be used to verify the authenticity and integrity of software and files before installation or execution.

52. Regular back up of critical data and systems must be implemented to ensure they can be restored in the event of a malware attack or data corruption.

53. A change management process to ensure that all software updates and configuration changes are reviewed, tested, and approved before implementation must be established.

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.