boston:college

INFORMATION SECURITY DATA PROTECTION POLICY: INFORMATION SECURITY POLICY

This policy is annually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Approved by: **Principal/CEO** Reviewed by: **Director of ICT**	
Date of next review	**July 2025**

This policy and procedure is subject to The Equality Act 2010 which recognises the following Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex, Sexual orientation and Disability.

1. Document Control

1.1. Document Details

Title	Information Security Policy
Author	Robbie Wallis / Claire Foster
Version	1.4
Date	Sept 2024
Status	Published

1.2. Revision History

Version	Date	Author	Comments
1.0	May 2021	Robbie Wallis	Definitive Release
1.1	May 2022	Robbie Wallis	Minor update to responsibilities
1.2	June 2023	Robbie Wallis / Claire Foster	Updated objectives
1.3	Dec 2023	Robbie Wallis	Amendment – BoxPhish completion rate
1.4	Sept 2024	Robbie Wallis / Claire Foster	Definitive Release – Target date specified in item 3 amended

1.3. Distribution

Name	Email	Organisation
All Staff	Uploaded to SharePoint	Boston College
All Learners and other interested parties	Post to college website	Boston College

INTRODUCTION

The organisation's Information Security Policy applies to all business functions within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment and people supporting these business functions. This document states the information security objectives and summarises the main points of the Information Security Policy.

PURPOSE

The purpose of information security is to ensure business continuity and minimise business damage by preventing and/or minimising the impact of security incidents. Information assets must be protected to ensure:

1. Confidentiality i.e., protection against unauthorised disclosure
2. Integrity i.e., protection against unauthorised or accidental modification
3. Availability as and when required in pursuance of the organisation's business objectives.

OBJECTIVES

1. To ensure all Boston College staff are fully aware of information security and their responsibilities towards it.
   - >80% of BoxPhish courses are to be completed within the current academic year.
   - >80% of staff will have completed data protection training.
   - >80% of staff will have completed online safety training.
   - Increasing trend and confidence to report weaknesses, events and incidents.
   - Regular updates to staff by email, BC Bulletin and other platforms.

2. To ensure all Boston College data is stored and handled appropriately maintaining their C.I.A.
   - 80% internal audit completed on time.
   - High risk incidents are investigated and resolved within 7 days.
   - Number of unaddressed CRITICAL and HIGH findings from penetration testing are resolved within 1 month.
   - Red risks to be monitored at each ISMS Committee, management reviews and accepted or actioned within 2 months.

3. To ensure all Boston College staff are aware of relevant legislation and its implications. To ensure Boston College is compliant with current legislation.
   - All staff to complete an appropriate induction that covers legislation.
   - Circulating guidance to staff when legislative changes occurs.
   - No penalties incurred.

*Targets to be achieved by 31st July 2025.

RESPONSIBILITIES

1. The Chief Executive has approved the Information Security Policy.

2. Overall responsibility for information security rests with the Director of ICT who will act as the ISMS Manager.

3. Day-to-day responsibility for procedural matters, legal compliance, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation and management reporting etc. rests with members of the ISMS Committee.

4. Day-to-day responsibility for data protection rests with the Data Protection Officers.

5. Day-to-day responsibility for technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations, rests with the ISMS Manager.

6. All employees or agents acting on the organisation's behalf have a duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay, direct to the ISMS representative. Employees attending sites that are not occupied by the organisation must ensure the security of the organisation's data and access their systems by taking particular care of laptop and similar computers and of any information on paper or other media that they have in their possession.

7. The ISMS Manager is responsible for drafting, maintaining, and implementing this Information Security Policy and similarly related documents.

8. As with other considerations including quality, financial, safeguarding and health & safety, information security aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the organisation.

9. The organisation's employees are advised and trained on general and specific aspects of information security, according to the requirements of their function within the organisation.

10. Adherence to information security procedures as set out in the organisation's various policies and guideline documents is the contractual duty of all employees and a clause to this effect is set out in the organisation's contracts of employment. The contract of employment includes a condition covering confidentiality regarding the organisation's business.

11. Copies of this management system, including the risk assessment (Annex A Statement of Applicability) are made available to all the organisation's employees.

12. Breach of the information security policies and procedures by the organisation's employees may result in disciplinary action, including dismissal.

13. In view of the organisation's position as a trusted provider of vocational and technical education services, particular care is taken in all procedures and by all employees to safeguard the information security of its service users and/or clients.

14. Agreements of 'Mutual Non-disclosure/Confidentiality' are entered into as appropriate with third party companies.

15. All statutory and regulatory requirements are met and regularly monitored for changes.

16. A Disaster Recovery/Business Continuity Plan is in place. This is maintained, tested and subjected to regular review by the ISMS Manager.

17. Further policies and procedures such as those for access, acceptable use of email and the internet, virus protection, backups, passwords, systems monitoring etc. are in place, maintained and are regularly reviewed by the ISMS Manager or an appointed representative, as appropriate.

18. This Information Security Policy is regularly reviewed and may be amended by the ISMS Manager to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the information security systems.

RELATED POLICIES

Policy Name	Summary
Access Control	Requirements that specify how access is managed and who may access information under what circumstances
Access to Guest Wi-Fi	Sets out requirements and responsibilities for accessing guest Wi-Fi at Boston College
Anti-Piracy	Details responsibilities for distribution of college software
CCTV	Details of how CCTV should be operated and accessed at Boston College
Clear Desk	Sets out the principles and requirement for data held in offices and classrooms
Cloud Computing	Outlines the acceptable use of cloud computing services
Computer Services Code of Conduct	These regulations cover the use of all computing facilities provided and administered by Boston College
Data Protection Policy	This sets out data protection principles and procedures for all data held by Boston College
Document and Data Retention	This sets out the principles and processes for data retention
Email and Internet	Details acceptable use of email and internet system
Information Classification	This policy outlines the classifications of data at Boston College along with the controls required
Network Systems Monitoring	Describes controls and procedures required for monitoring of the College network
Password Control	This sets out the requirements and controls for all user account passwords
Remote Access and Remote Working	This policy sets out additional principles, expectations and requirements relating to mobile and remote/home working
Rights of Individuals	Sets out the rights of individuals under the GDPR
Security Incident including Data Breach Reporting	Reporting process for security incidents and data breach

Software Procurement and Installation	Policy and procedure for staff procuring new software or installation of existing
Subject Access Request	Details the requirements and process for making a subject access request
User Account Creation	Describes the process for user account creation and deallocation
Virus Protection	Describes requirements for preventing and addressing computer viruses and malware on college systems

Date of Issue:	September 2024
Date of Next Review:	July 2025
Name:	Claire Foster and Robbie Wallis
Signed: