“Enabling Students to Accomplish their Academic Goal”

Information Security and Cybersecurity Policy

DOCUMENT CONTROL
Policy Number: BCP5
Version: 1.0
Date: March 2026
Owner: Head of IT
Approved by: Board of Directors
Next Review: March 2027

Address: 1st Floor, 9 Lymington Avenue, Wood Green N22 6EA
Email: info@bellmontcollege.co.uk
Tel: + 44 (0) 203 840 9294 + 44 (0) 203 929 7665
Website: www.bellmontcollege.co.uk
March 2026

Contents:

1. Introduction

Bellmont College is committed to protecting the confidentiality, integrity, availability and responsible use of information, digital services and technology used to support teaching, learning, assessment, student support, governance and administration. Information security is essential to student trust, staff confidence, academic continuity, lawful processing of personal data and the College's ability to deliver reliable higher education provision.

This policy brings together Bellmont College's information security policy requirements and its cybersecurity risk strategy in one implementation framework. It explains the controls expected of all users, how information and technology risks are identified and managed, and how oversight is exercised through College governance. It is written as a practical policy for staff, students, directors, contractors, partners and third parties, not only as a technical document for IT staff.

Bellmont College currently works with Liverpool Hope University as an awarding and academic partner. Under this partnership, students may use Bellmont College systems, local support services and learning resources while also accessing Liverpool Hope University systems, online resources, academic regulations and partnership procedures. Bellmont College is also seeking Office for Students approval for its own funding arrangements and wider institutional development. Future regulatory or funding developments may result in changes to governance, funding, systems, reporting and operational processes, however, Bellmont College continues to protect student interests, maintains continuity of study and manages information security risks transparently throughout any transition.

The policy retains and strengthens the existing Bellmont College information security requirements, including information classification, access control, endpoint security, network security, supplier assurance, incident management, business continuity, awareness training, audit and exceptions. It also develops a clearer cybersecurity risk strategy so that cyber, data, supplier, continuity, partnership and student-impact risks are recorded, owned, monitored and escalated through the College's committee structure.

2. Purpose of the Policy

The purpose of this policy is to establish a clear, institution-wide framework for protecting College information, technology, systems and digital services. It ensures that Bellmont College information is used lawfully, securely and appropriately, and that IT and cyber risks are managed in a way that protects students, staff, partners and the wider College community.

This policy aims to:

- protect information assets against unauthorised access, disclosure, modification, loss, destruction, misuse or disruption;
- protect students and staff by ensuring that systems used for teaching, learning, assessment, support, admissions, finance, registry and governance remain secure and available;
- establish an explicit cybersecurity risk strategy linked to the *(BCP2 Bellmont College Risk Management Policy)* and the *(BCP1 Bellmont College Risk Register)*;
- clarify how information security controls are implemented, monitored and reviewed through the Board of Directors, Senior Management Team, Academic Board, Quality Committee,

Student Experience Committee, Risk, Audit and Compliance Committee, Recruitment, Admissions and Registry Committee, Safeguarding and PREVENT Committee and Equality, Diversity and Inclusion Committee;
- support compliance with data protection, equality, consumer protection, higher education, cybersecurity and relevant criminal law requirements;
- support the current Liverpool Hope University partnership while maintaining Bellmont College's own institutional identity, governance and operational accountability;
- ensure that incidents, weaknesses and risks are reported promptly, investigated proportionately and used to improve controls.

This policy should be read alongside the *(BCP8 Bellmont College IT Acceptable Use Policy)*, (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy), *(BCP3 Bellmont College Business Continuity Plan)*, *(CAP1 Bellmont College Student Protection Plan and Policy)*, *(QGP1 Bellmont College Quality Handbook)* and *(BCP2 Bellmont College Risk Management Policy)*.

3. Regulatory and Legal Framework

Requirement	Relevance to this Policy
Office for Students Conditions C1, C2, C3 and C4	Support consumer protection, complaints scheme access, student protection and student protection directions where digital services affect students.
Office for Students Conditions E1, E2 and E3	Support governance, management and accountability for information security and cybersecurity risk.
Higher Education and Research Act 2017	Provides the higher education regulatory context for quality, standards, student interests, governance and accountability.
Competition and Markets Authority expectations	Support clear, accurate and accessible information, fair terms, transparent changes and fair complaints and redress.
UK Quality Code for Higher Education	Supports effective quality, standards, governance, resources, student engagement and enhancement.
UK GDPR and Data Protection Act 2018	Require lawful, fair, transparent and secure data processing, accountability, data breach management and data subject rights.

Equality Act 2010	Requires accessible, inclusive and non-discriminatory digital services, communications and monitoring.
Computer Misuse Act 1990	Applies to unauthorised access, unauthorised acts and system misuse.
Copyright, Designs and Patents Act 1988	Applies to lawful use of software, digital material, licensing and intellectual property.
Counter-Terrorism and Security Act 2015 and Prevent Duty guidance	Relevant to harmful extremist content and escalation.
Terrorism Act 2000, Fraud Act 2006, Malicious Communications Act 1988, Communications Act 2003 and Online Safety Act 2023	Relevant to digital conduct, misuse, fraud, harmful communications and illegal content.
Privacy and Electronic Communications Regulations, Regulation of Investigatory Powers Act 2000, Investigatory Powers Act 2016, Lawful Business Practice Regulations and Human Rights Act 1998	Inform monitoring, investigation, privacy and lawful business access to communications.
Office of the Independent Adjudicator Good Practice Framework	Relevant where IT or information security issues give rise to student complaints or redress matters.
Liverpool Hope University partnership requirements	Apply where Liverpool Hope University systems, data, student support, academic regulations or partnership obligations are involved.
ISO/IEC 27001, NIST Cybersecurity Framework and National Cyber Security Centre guidance	Provide good practice reference points used proportionately to Bellmont College's size, risk profile and operating model.

4. Scope of the Policy

This policy applies to all information created, received, stored, processed, transmitted or disposed of by or on behalf of Bellmont College, regardless of format, location or ownership of the device or system used. It applies to physical records, electronic records, email, cloud platforms, virtual learning environments, management information systems, finance systems,

admissions records, assessment information, student support records, HR information, governance records and any other College information asset.

This policy applies to:

- all employees, including permanent, temporary, casual, visiting, agency and contract staff;
- all students, applicants and former students where their accounts, records or complaints remain active;
- directors, committee members and external advisers;
- contractors, consultants, suppliers, visitors and third parties who access College information or systems;
- academic partners and service providers acting on behalf of Bellmont College;
- users of Bellmont College devices, networks, systems, software, accounts, cloud services, telephony, storage, printers, learning platforms and shared data repositories;
- users accessing Bellmont College information from home, off-site, mobile, personal or third-party environments;
- users accessing Liverpool Hope University systems or resources as part of Bellmont College partnership activity, where the relevant Liverpool Hope University policies and regulations also apply.

Where Liverpool Hope University systems, accounts or platforms are used, users must comply with both this policy and the relevant Liverpool Hope University requirements, including the *(LHU Liverpool Hope University Information Security Policy)* and the *(LHU Liverpool Hope University IT Facilities Acceptable Use Policy)*. Where requirements differ, the stricter or more protective requirement should normally be followed unless a formal partnership decision states otherwise.

5. Definitions

Term	Meaning
Information asset	Any data, record, system, application, service, device, account, network, process or repository of value to Bellmont College.
Confidentiality	Ensuring that information is only accessed, used or shared by people who are authorised to do so.
Integrity	Maintaining the accuracy, completeness and reliability of information and systems.
Availability	Ensuring that authorised users can access information and systems when required for legitimate College purposes.
Personal data	Information relating to an identified or identifiable person, as defined by UK GDPR.
Special category data	Sensitive personal data requiring additional protection, including health, disability, ethnicity, religion, biometric and other protected data categories defined in UK GDPR.
Information security incident	Any actual or suspected event that compromises or may compromise confidentiality, integrity, availability, legal compliance, student protection or operational continuity.

Term	Meaning
Cyber risk	The possibility of harm arising from failure, misuse, compromise or disruption of digital systems, networks, accounts, devices, data or services.
Risk owner	The person responsible for managing a risk, maintaining controls, reporting progress and escalating concerns when needed.
Third party	Any external supplier, contractor, partner, consultant or service provider that handles College information or provides systems or services to the College.
Privileged access	Elevated access that allows a user to administer, configure, monitor or control systems, accounts, data or security settings.

6. Core Information Security and Cybersecurity Principles

Bellmont College applies a risk-based, proportionate and student-focused approach to information security. The purpose is not to restrict legitimate teaching, learning or administrative activity unnecessarily, but to ensure that information and systems are protected in a way that is lawful, fair, practical and aligned with the College's obligations.

The following principles apply across this policy:

- confidentiality, integrity and availability must be considered in all system, data, supplier and operational decisions;
- personal data must be processed lawfully, securely and transparently in accordance with the (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy);
- access must be based on least privilege, need-to-know and role-based authorisation;
- systems and data must be designed, procured, configured, monitored and reviewed with security and privacy built in from the start;
- cybersecurity and IT risks must be recorded, assessed, owned and reviewed through the *(BCP1 Bellmont College Risk Register)*;
- student impact must be considered when systems, data, platforms or cybersecurity issues could affect teaching, learning, assessment, admissions, support, complaints or continuation of study;
- security controls must be proportionate, accessible and inclusive, and must not create avoidable barriers for disabled students, staff or other users who require reasonable adjustments;
- incidents and weaknesses must be reported promptly and used as opportunities for improvement rather than hidden or managed informally;
- partnership systems and Liverpool Hope University-related requirements must be managed clearly so that users understand which policies, accounts, services and escalation routes apply;
- security responsibilities belong to all users, not only to the IT team.

7. How this Policy Protects Students, Staff and College Operations

Information security is easiest to understand when viewed through the digital and student journey. The following table summarises how this policy works in practice.

Stage / area	What users can expect	Implementation route
Enquiry, recruitment and admissions	Applicants should be able to use safe, accurate and reliable online information, application processes and communications.	Website and admissions system controls; information checks; *(QGP6 Bellmont College Information Governance, Public Information and Transparency Policy)*; *(RAP1 Bellmont College Recruitment, Selection and Admission Policy)*.
Enrolment and account creation	Students should receive secure access to approved systems, clear digital expectations and support for logging in safely.	Identity checks; account creation controls; induction; *(BCP8 Bellmont College IT Acceptable Use Policy)*; student support signposting.
Teaching, learning and assessment	Students should be able to access learning platforms, resources, assessment information and feedback securely and reliably.	VLE access controls; learning resource review; Academic Board and Quality Committee oversight; *(QGP1 Bellmont College Quality Handbook)*.
Student support and wellbeing	Sensitive support, wellbeing, safeguarding and reasonable adjustment information should be handled confidentially and securely.	Restricted access; data protection controls; safeguarding escalation; *(SWP4 Bellmont College Mental Health and Wellbeing Policy)*; *(HSP1 Bellmont College Safeguarding and PREVENT Policy)*.
Digital disruption or cyber incident	Students should receive timely information, continuity arrangements and support where a system outage or cyber incident affects study.	Incident response; business continuity; student protection; *(BCP3 Bellmont College Business Continuity Plan)*; *(CAP1 Bellmont College Student Protection Plan and Policy)*.
Complaints and redress	Students and staff should have routes to raise concerns about IT access, digital service failure, monitoring or information security decisions.	Complaint handling; committee trend review; *(CAP3 Bellmont College Complaint and Appeal Policy and Procedure)*.
Partnership delivery with Liverpool Hope University	Students using Liverpool Hope University systems should be signposted to relevant Liverpool Hope University rules while Bellmont College maintains local support and escalation.	Partnership coordination; Liverpool Hope University system guidance; *(LHU Liverpool Hope University Information Security Policy)*; *(LHU Liverpool Hope University IT Facilities Acceptable Use Policy)*.

8. Information Security, Cybersecurity and IT Risk Strategy

Bellmont College's cybersecurity risk strategy is to identify, assess, control, monitor and escalate information security and digital risks in a way that protects students, staff, data, systems, academic continuity and institutional reputation. The strategy links this policy to the *(BCP2 Bellmont College Risk Management Policy)*, the (BCP1 Bellmont College Risk Register, the *(BCP3 Bellmont College Business Continuity Plan)* and the *(CAP1 Bellmont College Student Protection Plan and Policy)*.

The College's strategic objectives for cybersecurity and IT risk management are to:

- maintain reliable and secure systems for teaching, learning, assessment, student support, admissions, registry, finance, HR and governance;
- reduce the likelihood and impact of cyber incidents, data breaches, unauthorised access, system outages, supplier failures and partnership system failures;
- ensure that all material cybersecurity and IT risks have a named owner, clear controls, action plans, target dates and committee oversight;
- integrate cybersecurity and IT risk into academic quality, student protection, business continuity, safeguarding, equality and operational planning;
- support innovation, digital learning and artificial intelligence where risks are understood, controlled and reviewed;
- maintain clear escalation routes to the Senior Management Team and Board of Directors for high or critical risks;
- use incidents, audits, near misses, vulnerability findings and student feedback to strengthen controls.

8.1 Risk appetite

Bellmont College has a low appetite for information security risks that could cause unlawful processing of personal data, serious data loss, unauthorised access to confidential or restricted information, avoidable disruption to teaching or assessment, harm to students or staff, breach of safeguarding or Prevent duties, significant non-compliance, or loss of confidence in the College. The College has a controlled appetite for digital innovation where benefits to teaching, learning or operations are clear and where risks are assessed, mitigated, documented and monitored.

8.2 Risk categories

IT and information security risks will normally be considered under the following categories:

- cybersecurity risks, including malware, phishing, ransomware, compromise of accounts, vulnerability exploitation and denial of service;
- data protection and confidentiality risks, including unauthorised disclosure, loss, excessive access, insecure sharing, retention failures and breach notification risks;
- availability and continuity risks, including outages, disaster recovery failures, backup failures and loss of critical platforms;
- student protection risks, including disruption to teaching, learning, assessment, support, admissions, complaints or access to Liverpool Hope University online resources;
- supplier and cloud risks, including weak contract controls, insecure hosting, poor incident reporting, data transfer risks and service failure;
- partnership risks, including unclear responsibilities between Bellmont College and Liverpool Hope University, shared data handling, account access or system escalation issues;
- people risks, including insufficient awareness, poor password practice, social engineering, staff changes, insider threat and inadequate training;
- physical and environmental risks, including theft, loss, premises access, power interruption, fire, flood or insecure disposal;

- regulatory and legal risks, including failure to comply with data protection, equality, consumer protection, OfS, CMA, Liverpool Hope University or contractual requirements.

8.3 Risk assessment and scoring

Information security risks will be assessed by considering likelihood, impact, existing controls, residual risk, student impact, legal impact, operational impact and reputational impact. Bellmont College uses a proportionate scoring approach aligned with the *(BCP2 Bellmont College Risk Management Policy)*.

Element	How it is used
Likelihood	How probable the risk is, considering threat intelligence, past incidents, control maturity, supplier reliability and operational change.
Impact	The potential harm to students, staff, personal data, systems, academic continuity, finance, partnership obligations, reputation or regulatory compliance.
Residual risk	The level of risk remaining after current controls have been considered.
Treatment plan	The actions needed to reduce, transfer, avoid or formally accept the risk, including owner and target date.
Escalation level	The committee or senior owner responsible for oversight, depending on severity and impact.

8.4 Risk register and escalation

All material IT, cyber, data, supplier, Liverpool Hope University partnership and continuity risks must be recorded in the *(BCP1 Bellmont College Risk Register)*. The risk entry should identify the risk description, causes, consequences, controls, rating, owner, actions, review date and escalation route. High or critical risks must be escalated to the Senior Management Team and, where the risk could affect students, finances, regulatory compliance, partnership delivery or reputation, to the Board of Directors. Student-impacting risks must also be reported to the Academic Board, Quality Committee or Student Experience Committee where relevant.

8.5 Risk treatment and control improvement

Risk treatment may include technical controls, process changes, staff training, supplier contractual requirements, changes to access rights, enhanced monitoring, business continuity measures, additional student support, Liverpool Hope University partnership escalation, insurance, transfer arrangements or formal risk acceptance. Risk acceptance must be documented, time-bound, approved at the correct level and reviewed regularly.

9. Information Assets, Classification and Handling

Bellmont College identifies and manage information assets in proportion to their importance, sensitivity and risk. Each core information asset should have an owner responsible for access approval, accuracy, retention, security controls and review. Asset ownership should be recorded for key systems, including student records, admissions data, assessment information, finance records, HR records, governance records, safeguarding information and cloud services.

Information should be classified using the following framework. The classification should guide storage, sharing, access, retention and disposal.

Classification	Description	Examples
Public	Information approved for public release.	Website content, published policies, prospectus information, approved marketing material.
Internal	Information for College use that is not intended for public release.	Internal procedures, meeting papers, staff communications, working documents.
Confidential	Sensitive information requiring restricted access and controlled sharing.	Student records, assessment materials, HR files, complaints, financial records, partnership data.
Restricted	Highly sensitive information requiring strict need-to-know access and enhanced controls.	Authentication credentials, special category personal data, safeguarding records, incident reports, legal advice, high-risk breach records.

Users must store and share information using College-approved systems. Confidential or restricted information must not be stored on personal devices, personal email accounts, unapproved cloud storage or removable media unless specifically authorised and protected. Secure disposal must be used when information is no longer required, in line with the the (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy).

10. Identity, Account and Access Management

Access to Bellmont College information and systems must be controlled by identity, role, legitimate need and least privilege. Accounts must be created, changed and disabled through approved processes so that access remains appropriate throughout the user lifecycle.

The following requirements apply:

- each user must have a unique account wherever possible; shared accounts are prohibited unless formally approved, documented and controlled;
- strong passwords and multi-factor authentication must be used where required, especially for privileged access, remote access and access to confidential or restricted data;
- access must be authorised by the relevant manager, system owner or responsible College officer;
- access must be reviewed at least every six months for critical systems and promptly when a person changes role, leaves the College or no longer requires access;
- privileged accounts must be limited to authorised and trained users, logged, monitored and reviewed regularly;
- accounts must be disabled promptly when staff, students, contractors or third parties leave, withdraw, complete their role or no longer require access;

- Liverpool Hope University accounts and permissions must be managed in accordance with Liverpool Hope University requirements and partnership arrangements where students or staff access Liverpool Hope University systems.

Any suspected compromise of an account must be reported immediately to the Bellmont College IT Services at itsupport@bellmontcollege.co.uk. Users must never share passwords, authentication codes, access tokens or approval links with any other person.

11. Acceptable Use and Digital Conduct

All users must use College information and systems responsibly, lawfully and for authorised academic, administrative, professional or support purposes. Detailed user conduct requirements are set out in the *(BCP8 Bellmont College IT Acceptable Use Policy)*, which should be read alongside this policy.

Users must:

- use College systems for legitimate teaching, learning, assessment, student support, administration, governance, professional development or approved business purposes;
- protect credentials and report any suspected misuse or compromise;
- use professional, respectful and inclusive communication in digital environments;
- respect copyright, software licensing, confidentiality and intellectual property requirements;
- avoid accessing, creating, storing, downloading or sharing unlawful, harmful, offensive, discriminatory, extremist, defamatory or harassing material;
- avoid unauthorised scanning, testing, hacking, interception, bypassing of controls, malware use or any attempt to gain unauthorised access;
- use Liverpool Hope University systems, online resources and networks in accordance with Liverpool Hope University rules where those systems are accessed as part of the partnership.

Breaches may be managed under the *(HRP3 Bellmont College Staff Grievance and Disciplinary Policy)*, the *(QGP4 Bellmont College Student Handbook)*, the *(CAP3 Bellmont College Complaint and Appeal Policy and Procedure)*, Liverpool Hope University procedures where applicable, or referral to external authorities where required.

12. Endpoint, Mobile Device, BYOD and Remote Working Security

Devices used to access College information must be secure, supported and appropriate for the sensitivity of the information being accessed. This includes College-owned laptops, desktops, mobile phones, tablets, personal devices used under bring-your-own-device arrangements, remote working equipment and third-party devices approved for College purposes.

The following controls apply:

- College devices must run supported operating systems, approved endpoint protection, active firewall controls, encryption where appropriate and current security updates;
- personal devices may only access College systems where they meet minimum security requirements and where access is authorised;
- confidential or restricted data must not be stored locally on personal devices unless a documented exception has been approved and appropriate encryption is in place;

- mobile devices used for College work must be protected by passcode, biometric or password controls and must lock automatically after inactivity;
- lost or stolen devices must be reported immediately to the IT Service Desk and, where personal data may be affected, to the Data Protection Officer;
- users must not allow family members, friends or other unauthorised persons to use College devices or access College systems;
- remote working must use approved access methods, secure networks and suitable privacy safeguards, especially when handling student, HR, finance, safeguarding or assessment information;
- removable media must be avoided where possible and encrypted where use is authorised.

13. Network, Email and Communications Security

Bellmont College operates network, email and communications services in a way that supports reliable learning, teaching, administration and governance while reducing cyber and information security risk.

Bellmont College uses proportionate controls including:

- segmentation or separation of staff, student, guest, administrative and restricted services where practicable;
- firewalls, secure configuration, secure remote access, anti-malware, email filtering and phishing protection;
- monitoring of critical systems and logs to identify misuse, compromise, malicious activity or operational failure;
- secure wireless access with appropriate authentication and encryption;
- restrictions on unauthorised devices, rogue access points, unauthorised network services and insecure configurations;
- encryption or approved secure transfer methods for sensitive information in transit;
- controls over external email forwarding, bulk email, unsolicited communications and transmission of confidential or restricted data.

itsupport@bellmontcollege.co.ukUsers must take care when opening links, attachments or requests for information. Suspected phishing, social engineering or fraudulent requests must be reported immediately to the Bellmont College IT Services at . Where Liverpool Hope University networks or systems are accessed, users must comply with the *(LHU Liverpool Hope University IT Facilities Acceptable Use Policy)*.

14. Cloud Services, Suppliers, Data Sharing and Partnership Systems

Cloud services, suppliers and partnership systems are essential to College operations, but they introduce risks relating to data security, service continuity, jurisdiction, subcontracting, contractual control and incident response. Bellmont College will assess suppliers and systems before use and will maintain proportionate assurance throughout the relationship.

Before a supplier or cloud service handles College information, the responsible owner must consider:

- the type and sensitivity of information being processed;

- security controls, certifications, hosting location, backup arrangements and incident response commitments;
- data protection role, lawful basis, data processing agreement and international transfer safeguards where required;
- availability requirements, service levels, resilience and exit arrangements;
- contract clauses covering confidentiality, security, breach notification, audit, deletion, subcontracting and continuity;
- whether the service is compatible with College policies and Liverpool Hope University partnership obligations;
- student impact if the supplier fails, withdraws, changes terms or suffers a security incident.

Where information is shared with Liverpool Hope University, awarding bodies, regulatory bodies, professional advisers or service providers, the sharing must be lawful, necessary, secure and documented. The (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy), *(RAP2 Bellmont College Student Contract)*, *(CAP1 Bellmont College Student Protection Plan and Policy)* and the Partnership Agreement with Liverpool Hope University should be followed where relevant.

15. Data Protection, Privacy and Confidentiality

Information security and data protection are closely connected. Bellmont College must process personal data lawfully, fairly, transparently and securely. Users must only access personal data where they have a legitimate role-related need and must handle it in accordance with the (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy).

Data protection by design and by default must be considered when new systems, processes, reports, integrations or data-sharing arrangements are introduced. Data Protection Impact Assessments must be completed for high-risk processing, including processing involving sensitive student support information, safeguarding information, large-scale monitoring, new technologies or significant changes to digital services.

Committee papers, risk records, complaints, appeals, safeguarding records, wellbeing information, special consideration information, HR matters and data breach documentation must be handled confidentially. Access must be restricted and papers must be stored, shared and retained securely. Where a data breach is suspected, the Data Protection Officer must be informed immediately so that regulatory and individual notification obligations can be assessed.

16. Vulnerability, Patch, Configuration and Change Management

Systems must be kept secure throughout their lifecycle. Bellmont College applies risk-based controls for vulnerability management, patching, secure configuration, change approval and testing. These controls are intended to reduce the likelihood of compromise and prevent avoidable disruption to students and staff.

The College will:

- maintain an inventory of critical systems and information assets;

- apply security updates within timeframes proportionate to risk, criticality and operational impact;
- prioritise critical vulnerabilities, internet-facing systems, identity systems, systems containing confidential or restricted information, and systems supporting teaching, assessment or student services;
- test significant changes before release where practicable and record approval for changes to critical systems;
- separate development, testing and production environments where practicable;
- prevent unauthorised software installation and remove insecure or unlicensed software;
- review configuration standards for key systems, accounts, devices, firewalls and cloud services;
- consider student impact and business continuity before planned changes that may affect access to learning, assessment, admissions or support.

Changes that may affect Liverpool Hope University systems, partnership delivery or shared data must be coordinated with Liverpool Hope University through the appropriate partnership route. Significant academic delivery changes must also follow the *(QGP1 Bellmont College Quality Handbook)* and relevant Liverpool Hope University quality processes where applicable.

17. Logging, Monitoring, Investigation and Privacy Safeguards

Bellmont College may log, monitor and audit the use of College systems, networks, devices, email, cloud services and information assets for legitimate purposes, including security, system maintenance, legal compliance, safeguarding, incident response, business continuity and investigation of suspected misuse. Monitoring must be lawful, proportionate, necessary and consistent with privacy obligations.

Monitoring may include:

- system access logs and authentication records;
- network, firewall, endpoint, email and cloud security logs;
- file access, storage, sharing and printing activity;
- security alerts, vulnerability findings and malware detections;
- internet and email metadata, and content review only where lawful, authorised and necessary;
- administrative actions and privileged account use.

Monitoring records must be protected against unauthorised access, tampering or unnecessary disclosure. Access to monitoring records should be limited to authorised staff with a legitimate need. Where monitoring may affect staff or students, the College will act in accordance with the (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy), relevant privacy notices and the *(BCP8 Bellmont College IT Acceptable Use Policy)*.

18. Incident Management, Breach Reporting and Lessons Learned

All users must report suspected or confirmed information security incidents without delay. Prompt reporting enables the College to contain harm, protect students and staff, meet legal obligations and restore services. Users must not attempt to conceal incidents or investigate serious incidents independently without authorisation.

Reportable incidents include:

- loss, theft or unauthorised access to devices, accounts, documents or data;
- suspected phishing, malware, ransomware, social engineering or account compromise;
- accidental disclosure, misdirected email or inappropriate sharing of personal data;
- unauthorised software, system changes, network devices or cloud services;
- unexpected system behaviour, significant outage or unexplained data loss;
- access to illegal, harmful, extremist or safeguarding-related material;
- suspected breach of this policy, the *(BCP8 Bellmont College IT Acceptable Use Policy)* or Liverpool Hope University requirements.

Incidents will be triaged, contained, investigated, resolved and documented. Where personal data is involved, the Data Protection Officer will assess notification requirements. Where students may be affected, the Senior Management Team, Academic Board, Quality Committee, Student Experience Committee and Board of Directors will be informed at the appropriate level. Where Liverpool Hope University systems, accounts or partnership data are involved, Liverpool Hope University will be notified through the agreed partnership route. Lessons learned will be reviewed and actioned through committee oversight.

19. Incident Response Plan

Bellmont College maintains an Incident Response Plan to ensure that information security and cybersecurity incidents are reported, assessed, contained, investigated, resolved and reviewed in a timely and proportionate manner. The plan supports the College's wider obligations under the *(BCP6 Bellmont College Information Security and Cybersecurity Policy)*, (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy), *(BCP8 Bellmont College IT Acceptable Use Policy)*, *(BCP3 Bellmont College Business Continuity Plan)*, *(BCP2 Bellmont College Risk Management Policy and Risk Register)* and *(CAP1 Bellmont College Student Protection Plan and Policy)*.

An information security or cybersecurity incident may include:

- suspected or confirmed unauthorised access to College systems, accounts, devices or data;
- loss, theft or compromise of College equipment, records or information;
- phishing, malware, ransomware or social engineering attempts;
- accidental disclosure, loss or corruption of personal, confidential or restricted information;
- disruption to College systems, networks, email, cloud services, learning platforms or assessment systems;
- misuse of College IT resources, credentials or privileged access;
- supplier, partner or Liverpool Hope University system incidents that may affect Bellmont College students, staff, data, delivery or operations.

All users must report suspected incidents immediately to the Bellmont College IT Services at itsupport@bellmontcollege.co.uk and, where personal data may be involved, to the Data Protection Officer. Users must not attempt to investigate or resolve serious incidents

themselves unless specifically authorised to do so, as this may compromise evidence, increase risk or delay escalation.

The College will manage incidents using the following response stages:

Incident Response Plan:

Stage	Required response	Lead / escalation	Record / evidence
1. Report	Report immediately to IT Services at itsupport@bellmontcollege.co.uk and to the Data Protection Officer where personal data may be involved.	All users; IT Team; DPO	Incident report/email
2. Log and triage	Record key facts and assess severity, personal data risk, student/staff impact, continuity risk and escalation needs.	IT Team / Head of IT / DPO	Incident log; triage record
3. Contain	Limit harm by disabling accounts, isolating devices, blocking access, suspending services, preserving logs and notifying suppliers if needed.	IT Team / Head of IT / system owner	Containment log
4. Investigate	Confirm cause, scope, affected systems, affected users/data and legal, regulatory, partner or supplier obligations.	Head of IT / DPO / relevant senior staff	Investigation notes/evidence
5. Remediate	Remove malicious activity, fix vulnerabilities or misconfigurations, reset access and secure systems before normal use resumes.	IT Team / external support if required	Remediation record
6. Recover	Restore systems, data and services safely, prioritising teaching, learning, assessment, support, finance, payroll and essential communications.	IT Team / SMT	Recovery confirmation
7. Communicate	Inform staff, students, Liverpool Hope University, suppliers, regulators or stakeholders where appropriate, using clear and proportionate communication.	SMT / CEO / DPO	Communication record
8. Escalate	Escalate material incidents through SMT, Risk, Audit and Compliance, Quality Committee, Academic Board and Board of Directors as appropriate.	SMT / Head of IT / Head of Quality and Operations / Board of Directors	Committee reports/minutes
9. Review and learn	Review root causes, control weaknesses, training needs, policy updates, risk register changes and improvement actions.	Head of IT / DPO / SMT	Post-incident review; action tracker

Where an incident involves personal data, the Data Protection Officer will assess whether the incident constitutes a personal data breach and whether notification to the Information Commissioner's Office or affected individuals is required under UK GDPR and the Data Protection Act 2018. The College will keep appropriate records of the breach assessment, decisions taken, notifications made and actions completed.

Where an incident may affect teaching, assessment, student records, digital learning systems, submission arrangements, student support, partnership delivery or continuation of study, the Senior Management Team will coordinate with the Head of Quality and Operations, Head of Academic Programmes, Head of Professional Services, relevant programme teams and Liverpool Hope University where applicable. Temporary arrangements may include alternative communication channels, revised submission arrangements, adjusted access arrangements, alternative learning materials, extended deadlines, enhanced technical support or escalation under the *(CAP1 Bellmont College Student Protection Plan and Policy)*.

Material incidents must be escalated through the College's governance structure. The Senior Management Team will oversee operational response and resource decisions. The Risk, Audit and Compliance Committee will review the incident, risk controls and assurance evidence. The Quality Committee and Academic Board will consider any impact on academic delivery, assessment, student experience or quality assurance. The Board of Directors will receive assurance on significant incidents, regulatory implications, business continuity risks and completion of corrective actions.

The College will retain an incident record including the date reported, reporter, affected systems or data, severity rating, actions taken, communications issued, regulatory decisions, recovery steps, lessons learned and action owners. Incident records will be reviewed periodically to identify recurring issues, inform staff training, update the risk register and strengthen the College's information security and cybersecurity controls.

20. Business Continuity, Disaster Recovery and Student Protection

Information security is directly linked to business continuity and student protection. A cybersecurity incident, system outage, data loss, supplier failure or loss of access to digital learning resources may affect teaching, assessment, student support, admissions, complaints or continuation of study. Bellmont College will therefore manage major IT disruption through the *(BCP3 Bellmont College Business Continuity Plan)* and the *(CAP1 Bellmont College Student Protection Plan and Policy)*.

Critical systems must have proportionate continuity and recovery arrangements. These may include backups, recovery time objectives, alternative access routes, manual workarounds, communication plans, supplier escalation, Liverpool Hope University coordination, temporary learning arrangements, revised assessment arrangements, student support and mitigation where disruption affects students.

Backups of essential data must be protected, encrypted where appropriate, stored securely and tested periodically. Recovery arrangements should be reviewed after significant incidents, system changes, supplier changes, partnership changes or operational developments. Where disruption materially affects students, communications must be clear, timely and accessible, and any mitigation, complaint or redress routes must be explained.

21. Artificial Intelligence, Emerging Technology and Digital Learning Risk

Artificial intelligence and emerging technologies can support teaching, learning, administration and service improvement, but they can also create risks relating to confidentiality, data protection, bias, accuracy, academic integrity, intellectual property, transparency and over-reliance. AI and emerging technology must therefore be assessed before use for College business or student-facing activity.

Users must not enter personal data, confidential information, restricted information, safeguarding information, assessment materials, unpublished policy material or commercially sensitive information into public AI tools unless the use has been authorised and appropriate safeguards are in place. AI-generated content must be reviewed by a competent person before use in official communications, teaching materials, policies, student support, reporting or assessment-related work.

The use of AI by students in assessment must be managed in accordance with the *(Bellmont College Academic Integrity Policy)* and any applicable Liverpool Hope University academic regulations. Where a new AI system or digital learning tool is proposed, the risk assessment should consider data protection, equality, accessibility, academic quality, student information, supplier assurance and student protection impacts.

22. Physical and Environmental Security

Physical security supports information security. Equipment, records and spaces that process or store College information must be protected from unauthorised access, theft, loss, environmental damage and inappropriate disclosure.

The College will:

- restrict access to server, communications, storage and other sensitive areas to authorised persons;
- protect equipment from fire, flood, power failure, theft and environmental hazards as far as reasonably practicable;
- ensure visitors to restricted areas are authorised, supervised and recorded where appropriate;
- use secure disposal for redundant equipment, storage media and confidential paper records;
- require users to secure laptops, printed papers, portable media and mobile devices, especially when travelling or working remotely;
- ensure physical security risks are considered through the *(HSP2 Bellmont College Health and Safety Policy)*, *(BCP3 Bellmont College Business Continuity Plan)* and *(BCP1 Bellmont College Risk Register)*.

23. Security Awareness, Training and Culture

Information security depends on informed and responsible users. Bellmont College maintains a security-aware culture through induction, training, reminders, incident learning, phishing awareness, targeted support for higher-risk roles and communication of emerging threats.

Training will be proportionate to role and risk. It will include information security, data protection, acceptable use, phishing, password protection, remote working, incident reporting

and secure handling of personal data. Additional training may be provided to staff handling admissions, student records, safeguarding, wellbeing, finance, HR, assessment, complaints, system administration or governance papers.

Student-facing information will be provided in clear and accessible language. Where students or staff need alternative formats, support or reasonable adjustments to access digital services or security guidance, arrangements will be considered under the *(SWP2 Bellmont College Equality, Diversity and Inclusion Policy)* and the *(SWP1 Bellmont College Reasonable Adjustment and Special Considerations Policy)*.

24. Policy Exceptions and Risk Acceptance

Any exception to this policy must be exceptional, justified, risk-assessed, time-bound and approved by an appropriate senior owner. Exceptions must not be used to bypass controls for convenience or to avoid proper resourcing. The request must explain the business need, risks, compensating controls, duration, owner and review date.

Exceptions involving confidential or restricted information, personal data, student-impacting systems, safeguarding information, Liverpool Hope University systems, major suppliers or critical infrastructure must be escalated to the Head of IT / Information Security Lead and, where relevant, the Data Protection Officer, Senior Management Team or Risk, Audit and Compliance Committee. Accepted risks must be recorded in the *(BCP1 Bellmont College Risk Register)* where material.

25. Governance and Committee Implementation Framework

Information security and cybersecurity risk strategy are implemented through Bellmont College's governance and committee structure. The purpose of this structure is to ensure that risks are identified, acted on, monitored, evidenced and escalated. A security concern may arise from an incident, audit, vulnerability scan, student complaint, staff concern, supplier review, Liverpool Hope University partnership matter, system change, data breach, safeguarding concern or business continuity event. It should then move through the appropriate governance route until the action is complete and evidence is retained.

The implementation model is: identify the issue; assess the risk and student impact; assign an owner; agree corrective or preventive action; record the matter in the appropriate action log or risk register; report to the relevant committee; escalate material risks; close the action only when evidence shows that it has been completed. This mirrors the governance approach used in the *(CAP2 Bellmont College Consumer Protection Policy and Implementation Framework)* and links information security to student protection and institutional assurance.

Committee / body	How it implements this policy
Board of Directors	Receives assurance on significant cybersecurity and IT risks, cyber incidents, data breaches, business continuity, student protection, regulatory developments, Liverpool Hope University partnership risks and resourcing requirements.
Audit and Risk Committee	Advises the Board of Directors on audit, internal control, risk management, cybersecurity assurance, data protection risk, supplier assurance and business continuity controls.

Committee / body	How it implements this policy
Academic Committee	Maintains academic oversight where information security or cybersecurity risk affects academic standards, digital learning, learning resources, assessment, academic integrity or continuation of study.
Senior Management Committee	Coordinates operational implementation, resources, response to serious risks, business continuity, supplier issues, Liverpool Hope University partnership escalation, student communications and corrective actions.
Quality Committee	Monitors the relationship between information security, academic quality, student outcomes, complaints, student feedback, public information and quality assurance evidence.
Learning and Teaching Committee	Reviews digital learning, assessment support, learning resources, inclusive practice and teaching delivery issues where information security or system access affects students.
Recruitment, Admissions and Registry Committee	Monitors secure handling of applicant and student records, admissions systems, offer communications, enrolment records, attendance, engagement, registry data integrity and applicant complaints.
Student Staff Committee and Partnership Routes	Provides a student voice route for digital access, VLE, IT disruption, communication and support issues. Liverpool Hope University partnership matters are escalated through the relevant operational, academic and strategic partner routes where applicable.

25. Roles and Responsibilities

Role / body	Responsibility
Board of Directors	Retains ultimate governance oversight for information security, cybersecurity risk, regulatory compliance, institutional resilience and student protection.
CEO	Holds executive accountability for ensuring that information security, cybersecurity risk strategy, regulatory compliance and student protection are implemented effectively.
Head of IT / Information Security Lead	Owns day-to-day implementation of this policy, coordinates technical controls, maintains security standards, reports cybersecurity and IT risks and leads incident response with relevant colleagues.
Data Protection Officer	Advises on data protection law, DPIAs, breach assessment, data subject rights, privacy notices, data sharing and compliance with the (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy).
Head of Quality and Operations	Ensures policy implementation is linked to quality assurance, governance reporting, public information, evidence monitoring, student protection and partnership oversight.
Head of Academic Programmes	Ensures that digital learning, assessment, academic support, programme delivery and academic quality risks are reported and managed through academic governance.

Role / body	Responsibility
Head of Professional Services	Ensures that admissions, registry, finance, student support, HR and operational services follow information security and data handling requirements.
Heads of Department and managers	Ensure staff comply with this policy, approve appropriate access, identify information assets, report risks and support training and incident response.
System owners and information asset owners	Maintain ownership of specific systems or information assets, including access approval, accuracy, retention, risk assessment and supplier liaison.
Programme Coordinators and Module Tutors	Use digital learning and assessment systems appropriately, protect student information and escalate academic or student-impacting technology risks.
Student Support and Safeguarding staff	Protect sensitive wellbeing, safeguarding and reasonable adjustment information and escalate concerns using approved routes.
All staff, students and authorised users	Use systems responsibly, protect credentials, follow this policy, report incidents promptly and comply with the *(BCP8 Bellmont College IT Acceptable Use Policy)*.
Suppliers, contractors and third parties	Comply with contractual, data protection, security and confidentiality requirements and report incidents or weaknesses promptly.
Liverpool Hope University partnership contacts	Coordinate where Liverpool Hope University systems, data, policies, student support, academic regulations or partnership obligations are affected.

26. Conclusion

Bellmont College recognises that information security and cybersecurity risk management are fundamental to academic quality, student protection, lawful data processing, operational resilience and public trust. This policy sets out how Bellmont College protects information and digital services while supporting accessible, reliable and effective teaching, learning, assessment, student support and administration.

Through this policy, Bellmont College undertakes to manage information security and cybersecurity risks through clear ownership, proportionate controls, committee oversight, prompt incident reporting, student-focused business continuity and continuous improvement. Bellmont College continues to work with Liverpool Hope University under current partnership arrangements and manages any future OfS funding or regulatory changes carefully, transparently and in the interests of students.

Bellmont College Information Security and Cybersecurity Policy					
Version	**Date**	**Author(s)**	**Amendments**	**Approved by**	**Next review**
1	March 2026	Head of IT	New Document	Board of Directors	March 2027