“Enabling Students to Accomplish their Academic Goal”

IT Acceptable Use Policy

DOCUMENT CONTROL
Policy Number: BCP7
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 providing a safe, secure, inclusive and reliable digital environment for learning, teaching, assessment, student support, administration, governance and partnership delivery. This IT Acceptable Use Policy explains the expected standards of everyone who uses Bellmont College information technology resources and any partner or third-party digital services accessed through Bellmont College arrangements.

Bellmont College currently works with Liverpool Hope University as an academic and awarding partner. Students may use Bellmont College services alongside Liverpool Hope University systems, resources, regulations and academic oversight, depending on the programme and the applicable partnership arrangements. Bellmont College is also seeking Office for Students approval for its own funding arrangements. Future funding or regulatory approval may affect some processes, systems, reporting routes and responsibilities, but Bellmont College continues to protect student interests, maintain academic continuity and communicate any material changes clearly and fairly.

This policy therefore operates in the current Liverpool Hope University partnership context while being suitable for future development of Bellmont College governance, funding and regulatory arrangements. Where a student, staff member or authorised third party accesses Liverpool Hope University systems, they must comply with the applicable Liverpool Hope University digital policies, including the full policy names listed in this document.

The policy is sets out what users may and may not do, but it also explains how expectations are communicated, monitored, reported, governed and reviewed through Bellmont College committees and management arrangements.

2. Purpose of the Policy

The purpose of this policy is to protect students, staff, directors, visitors, College data, digital services and academic operations by setting clear rules for responsible and lawful use of IT resources. It supports the College in maintaining secure systems, protecting personal data, meeting regulatory duties and ensuring that digital services are used in ways that are consistent with Bellmont College values and student interests.

In practice, the policy is intended to:

- protect Bellmont College IT infrastructure, networks, devices, applications, cloud services, virtual learning environments, student records, College data and partner systems from misuse, disruption, damage or compromise
- support teaching, learning, assessment, academic integrity, student support, administration and governance through dependable digital services
- ensure that users understand their responsibilities when using Bellmont College or Liverpool Hope University systems, including email, learning platforms, student portals, online assessment tools and cloud services
- promote lawful, ethical, inclusive and respectful online behaviour

- support compliance with data protection, equality, safeguarding, Prevent, consumer protection, quality assurance and cybersecurity expectations
- explain how IT acceptable use is implemented through staff training, induction, access controls, incident reporting, governance committees, monitoring, audit and annual review
- provide fair and proportionate routes for responding to breaches, including access restrictions, support, investigation, disciplinary action and referral to external agencies where required.

3. Regulatory and Legal Framework

This section consolidates the main regulatory and legal requirements relevant to this policy. These requirements apply across all policy areas and are not repeated under every topic. Bellmont College interprets and apply this framework proportionately, taking account of its current partnership arrangements with Liverpool Hope University and any future changes arising from Office for Students approval, funding arrangements or regulatory status.

The policy has been developed with reference to the following regulatory, legal and sector requirements:

Requirement	Relevance to this Policy
Office for Students regulatory framework	Informs access, quality, student support, consumer protection, complaints, student protection, governance, accountability, transparency, data provision and financial support expectations.
Higher Education and Research Act 2017	Provides the statutory framework for regulation of higher education in England.
CMA and consumer protection law	Supports clear information, fair terms, transparent changes, fair complaints handling and protection of students when services change or fail.
UK Quality Code for Higher Education	Supports effective resources, student engagement, partnership, information, learning opportunities, assessment, complaints, appeals, monitoring and enhancement.
UK GDPR, Data Protection Act 2018 and PECR	Supports lawful, secure and transparent handling of personal data, privacy,

	security, data protection by design and breach reporting.
Equality Act 2010 and accessibility requirements	Supports non-discrimination, reasonable adjustments, accessible digital services and inclusive communication.
Computer Misuse Act 1990 and cyber-related law	Supports controls against unauthorised access, malware, harmful communications, fraud, illegal content and system misuse.
Copyright and intellectual property law	Supports lawful use of software, digital material, licences, learning resources and intellectual property.
Safeguarding, Prevent and online safety duties	Supports escalation of online safety, extremist content, welfare, harassment and safeguarding concerns.
Jisc, Janet, PCI DSS, supplier and partner requirements	Supports acceptable use of education networks, payment security, supplier controls and contractual digital requirements.
Liverpool Hope University partnership requirements	Apply where Liverpool Hope University systems, data, academic regulations, digital policies, student-facing policies or quality assurance arrangements are relevant to partnership delivery.

4. Scope of the Policy

This policy applies to everyone who is given access to Bellmont College IT resources or who uses partner digital services through Bellmont College arrangements. It applies whether the user is on campus, working remotely, studying online, using a College device, using a personal device or accessing cloud services from another location.

The policy applies to:

- all students and applicants who are given access to digital systems
- all employees, including permanent, temporary, part-time, sessional, casual and agency staff
- directors and members of College committees
- contractors, consultants, suppliers, placement providers, volunteers and visitors who are granted access to College IT resources

- Liverpool Hope University staff, where they access Bellmont College systems or data as part of partnership delivery
- Bellmont College users who access Liverpool Hope University IT facilities, Moodle, email, student records, University data, learning resources or other partner systems
- any other authorised person using College-owned, College-managed or partner-managed devices, accounts, networks, systems or data.

IT resources include, but are not limited to:

- desktop computers, laptops, tablets, mobile phones, printers, telephones and audio-visual equipment
- wired and wireless networks, internet access, firewalls, VPNs, remote access tools and network storage
- email, messaging, collaboration platforms, calendars, file sharing, cloud services and digital communication tools
- virtual learning environments, student portals, online libraries, digital attendance systems, assessment systems and academic records
- software, licensed applications, databases, artificial intelligence tools, online forms, payment systems and reporting tools
- personal devices used to access College or partner systems
- College data, partner data, personal data, confidential information, teaching materials, assessment materials, records and system logs.

The policy applies to all use of IT resources for college business, study, research, academic support, assessment, administration, governance and limited personal use permitted under this policy. It also applies to online conduct that affects Bellmont College, Liverpool Hope University, students, staff, partners, reputation, safeguarding, data protection or the safety and wellbeing of others.

5. How this Policy Protects Students, Staff and Services

Acceptable use is not only an IT requirement. It protects students' learning experience, staff working conditions, institutional reputation, data security, academic integrity, digital inclusion and continuity of study. The table below explains how this policy works in practice.

Area	What users can expect	Implementation route
Access and induction	Users receive clear information about IT expectations, passwords, email, online learning systems, data protection, accessibility and incident reporting.	Student induction; staff induction; IT account set-up; *(QGP3 Bellmont College Student Handbook)*; *(HRP2 Bellmont College Employee Handbook)*.

Area	What users can expect	Implementation route
Learning, teaching and assessment	Digital learning systems are used lawfully, securely and consistently so that students can access teaching, assessment, feedback and support.	Learning and Teaching Committee; Academic Committee; Quality Committee; programme monitoring; *(LTP6 Bellmont College Academic Integrity and Misconduct Policy)*.
Partner systems	Where Liverpool Hope University systems are used, students and staff follow the relevant University digital rules while Bellmont College provides local support and escalation.	Partnership management; Registry; IT Service Desk; *(LHU Liverpool Hope University IT Facilities Acceptable Use Policy)*; *(LHU Liverpool Hope University Information Security Policy)*.
Data protection and confidentiality	Personal data and confidential information are accessed only when needed, stored securely, shared lawfully and reported promptly if lost or compromised.	Data Protection Officer; Head of IT; Quality Committee; Audit and Risk Committee; *(BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy)*.
Cybersecurity and continuity	Cyber risks are managed through access controls, security monitoring, incident response, staff training, backups and business continuity planning.	IT incident management; Senior Management Committee; Board of Directors; *(BCP3 Bellmont College Business Continuity Plan)*; *(BCP2 Bellmont College Risk Management Policy)*.
Student voice and experience	Digital access, learning resources, online systems and accessibility concerns are monitored through student feedback and committee reporting.	Student Staff Committee; Student Staff Committee; Quality Committee; *(QGP5 Bellmont College Student Representative Handbook)*.
Safeguarding, equality and respectful conduct	Online behaviour must be respectful, inclusive and safe. Safeguarding, harassment, discrimination and PREVENT concerns are escalated quickly.	Safeguarding and Prevent Committee; Equality, Diversity and Inclusion Committee; Student Support; *(HSP1 Bellmont College Safeguarding and PREVENT Policy)*; *(SWP2 Bellmont College Equality, Diversity and Inclusion Policy)*.

Area	What users can expect	Implementation route
Complaints, concerns and redress	Users can raise concerns about IT access, digital services, online behaviour, learning resources or data issues through appropriate routes.	IT Service Desk; Student Support; complaints monitoring; *(CAP3 Bellmont College Complaint and Appeal Policy and Procedure)*.

6. Core Acceptable Use Principles

All users must use IT resources responsibly, lawfully, respectfully and proportionately. The following principles apply to every section of this policy and to all Bellmont College or partner systems used through Bellmont College arrangements.

Lawful use: Users must comply with UK law, regulatory obligations, partner requirements and College policies. Users must not use IT resources to commit, encourage, conceal or facilitate unlawful activity.

Student interests and continuity: IT decisions protect students' access to learning, assessment, support, communication and records wherever reasonably possible. If a system failure or security incident affects students, the College provides clear communications and mitigation.

Security by default: Users must protect accounts, devices, data and systems. The College uses proportionate technical and organisational controls to reduce risk and support safe access.

Need-to-know access: Users may only access data, systems or records for which they have a legitimate College, academic, support or partnership purpose.

Respect and inclusion: Digital communication must be respectful and must not discriminate, harass, bully, intimidate, defame, threaten or exclude others.

Accuracy and professionalism: Users must take reasonable care that information they create, send, upload or publish through College systems is accurate, professional and appropriate to the context.

Accountability: Users are responsible for activity carried out using their accounts. Committees and managers are responsible for ensuring that policy implementation is recorded, monitored and reviewed.

Proportionality and privacy: Monitoring and investigation is carried out only for legitimate purposes and in a lawful, proportionate and accountable way.

7. Access, Eligibility and Identity Management

Access to Bellmont College IT resources is provided to support College business, study, teaching, assessment, student support, governance and authorised partnership activity. Access is a privilege linked to a legitimate role or student status and may be restricted,

suspended or withdrawn where required for security, safeguarding, data protection, disciplinary, contractual or operational reasons.

Eligible users normally include:

- current students enrolled on a programme or given access for a pre-enrolment purpose
- current staff and authorised workers with a legitimate work-related need
- directors and committee members who require access to papers, systems or College communications
- contractors, consultants, suppliers, visitors or partner staff who have been approved for a defined purpose and period
- Liverpool Hope University staff or authorised representatives where access is needed for academic partnership, quality assurance, student support or regulatory purposes.

The following users must not retain access unless formal approval has been granted for a defined reason, scope and period:

- former students
- former staff
- members of the general public
- contractors, consultants or visitors after the approved access period has ended
- any user whose access has been suspended or withdrawn under this policy or another relevant procedure.

The IT Team maintains account creation, amendment and closure processes. Managers and Registry must notify IT promptly when a user joins, changes role, changes programme, suspends study, withdraws, completes study, leaves employment or no longer requires access. Access to sensitive systems must be granted using role-based permissions and reviewed periodically.

Where a user accesses Liverpool Hope University systems, the user must comply with the applicable Liverpool Hope University access rules and policies, including *(LHU Liverpool Hope University IT Facilities Acceptable Use Policy)*, *(LHU Liverpool Hope University Information Security Policy)*, *(LHU Liverpool Hope University Data Protection Policy)*, *(LHU Liverpool Hope University Portable Data Device Security Policy)*, *(LHU Liverpool Hope University Wireless Service Protocol)* and *(LHU Liverpool Hope University E-mail Policy)*.

8. Acceptable Use

IT resources are provided primarily for legitimate College, academic, administrative and partnership purposes. Limited personal use may be permitted where it is reasonable, lawful, non-commercial, does not interfere with College work or study, does not consume excessive resources and does not breach this policy.

Acceptable use includes:

- teaching, learning, assessment and academic support
- research, scholarship and professional development
- student support, wellbeing, accessibility and reasonable adjustment activity
- programme administration, admissions, registry, finance, quality assurance and governance
- approved communication with students, applicants, staff, directors, partners, suppliers and regulators
- approved use of Liverpool Hope University systems and resources for partnership delivery
- approved online meetings, collaboration, digital resources, virtual learning environments and cloud services
- approved use of assistive technology and accessibility tools
- limited personal use that is lawful, proportionate, non-commercial and does not create risk or disruption.

Users must treat as confidential any information, records, software, credentials, assessment material or College or partner data that becomes available to them accidentally. Such information must not be copied, retained, modified, disclosed, distributed or used. The user must report the matter promptly to the IT Service Desk and, where personal data is involved, to the Data Protection Officer in line with *(BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy)*.

Users must pay any authorised charges arising from their use of IT resources where charges are published or agreed, for example printing, replacement equipment, specialist software or recoverable costs connected with misuse.

9. Unacceptable Use

The following activities are prohibited. The list is not exhaustive. A user must not use Bellmont College or partner IT resources in any way that is unlawful, unsafe, discriminatory, disruptive, dishonest, unauthorised, commercially exploitative, reputationally damaging or inconsistent with College policies.

9.1 Illegal, harmful or offensive activity

- accessing, creating, downloading, storing, transmitting or distributing illegal material, including child sexual abuse material, terrorist content, extremist material, obscene material or material that promotes hatred or violence
- committing or attempting to commit unauthorised access, hacking, phishing, malware distribution, denial-of-service activity, credential theft, fraud or any other offence under the Computer Misuse Act 1990 or related law
- creating, sending, uploading or sharing material that is sexist, racist, homophobic, transphobic, ableist, defamatory, threatening, harassing, bullying, obscene, malicious or discriminatory
- using systems to stalk, intimidate, exploit, coerce, groom, radicalise, impersonate or deceive another person

- accessing extremist, terrorist or harmful material except where expressly authorised for legitimate academic or safeguarding purposes and subject to appropriate risk controls
- using IT resources for gambling, cryptocurrency mining, unauthorised gaming, unlawful file sharing, unauthorised commercial activity or personal financial gain.

9.2 Security misuse

- attempting to gain unauthorised access to systems, accounts, data, devices, networks or services
- sharing passwords, authentication codes, security tokens, access cards or credentials with another person
- using another person's account or allowing another person to use an account assigned to the user
- disabling, bypassing or interfering with security controls, firewalls, antivirus software, monitoring tools, access controls, web filters, patching, encryption or device management
- scanning, probing, testing or monitoring networks or systems without written IT approval
- intercepting, eavesdropping on, recording or monitoring network traffic or communications without authorisation
- connecting unauthorised devices, servers, routers, wireless access points, storage devices or Internet of Things equipment to College networks
- introducing malware, spyware, ransomware, viruses, worms, keyloggers, hacking tools, credential harvesters or other harmful software
- continuing to use software, hardware or a device after IT has instructed the user to stop because it creates risk or disruption.

9.3 Misuse of information, copyright and resources

- accessing, copying, changing, deleting, disclosing or sharing data without a legitimate need and authorisation
- copying, downloading, uploading, distributing or using copyright material, software, images, video, audio, datasets or teaching material without permission, licence or lawful exception
- using unlicensed software, unauthorised cloud storage, unauthorised file sharing or unsupported applications for College business
- sending unsolicited bulk messages, chain messages, spam, misleading communications or unauthorised marketing
- deliberately wasting IT resources, including excessive printing, avoidable storage consumption, unnecessary bandwidth use or actions that degrade services for others
- using IT resources in a way that denies service to other users or disrupts the work of students, staff, partners or the College.

9.4 Conduct affecting reputation or community safety

- using Bellmont College or Liverpool Hope University systems, branding, email addresses, social media or digital resources in a way that brings either institution into disrepute
- misrepresenting personal views as official College or partner views
- publishing confidential College, student, staff, partner or third-party information without authorisation
- creating, transmitting or publishing content that breaches the dignity, privacy, rights, safety or wellbeing of others
- breaching the terms of service or community standards of a digital platform used for College business or study.

10. Account Security and Passwords

Account security is essential because access to College and partner systems may provide access to personal data, teaching material, assessment information, finance information, safeguarding records, student records and confidential communications. Users are responsible for protecting their credentials and devices.

Users must:

- keep usernames, passwords, passphrases, PINs, authentication codes and security tokens confidential
- use strong passwords or passphrases that comply with College password standards
- change passwords immediately and report the matter if compromise is suspected
- use multi-factor authentication where it is required or available
- avoid reusing College passwords on personal, social media or other external accounts
- lock screens or log out when devices are unattended
- not store passwords in browsers, spreadsheets, notes, unencrypted files or visible locations
- not approve authentication prompts that they did not initiate
- notify the IT Service Desk immediately if a device, account, authentication method or security token is lost, stolen or compromised.

Managers, tutors and support staff must not ask a user to disclose a password. IT support must use approved support tools and identity verification processes rather than asking for passwords.

11. Email, Messaging and Electronic Communications

College email and approved communication systems must be used professionally and consistently. They form part of the formal record of College and student communication and may be needed for academic, regulatory, contractual, safeguarding, complaints, data protection or governance purposes.

Users must:

- use College or approved partner email accounts for official College business and student communication
- avoid using personal email accounts for College business, especially where personal data, confidential information or assessment information is involved
- use professional, respectful and clear language in all electronic communications
- check recipients carefully before sending messages or attachments
- use approved email signatures and role-based mailboxes where required
- be alert to phishing, malware, suspicious links, unexpected attachments, impersonation and social engineering
- report suspicious emails to the IT Service Desk and avoid forwarding them to others unless instructed by IT
- not auto-forward College email to external accounts without IT approval
- not send confidential or personal data using insecure methods where safer alternatives are available
- not use College messaging tools for harassment, bullying, discrimination, unauthorised political campaigning, commercial advertising or spam.

Where Liverpool Hope University email, Moodle or other communication systems are used for partnership delivery, users must also follow *(LHU Liverpool Hope University E-mail Policy)*, *(LHU Liverpool Hope University IT Facilities Acceptable Use Policy)* and *(LHU Liverpool Hope University Student Guide to Regulations and Policies)*.

12. Internet, Web, Networks, Wi-Fi and Partner Systems

Internet and network access is provided for learning, teaching, assessment, administration, research, professional development, student support and limited personal use. Bellmont College may apply filtering, security controls, network segmentation, logging and access restrictions to protect users and systems.

Users must:

- not attempt to bypass web filtering, security controls, network access controls, VPN controls or geographic restrictions
- not access websites or services that are illegal, harmful, discriminatory, extremist, malicious, sexually exploitative, fraudulent or inappropriate for the College environment
- not download or install software, plugins, browser extensions, scripts or tools unless approved by IT
- exercise caution when entering personal, financial or College information into websites or online forms
- not run personal servers, unauthorised wireless access points, peer-to-peer sharing services, mining software or network scanning tools
- not connect equipment that could disrupt the network or create an unmanaged security risk

- follow any local rules for specialist classrooms, labs, online examinations, digital assessments, loan devices and printing.

When a user accesses another network through Bellmont College, Liverpool Hope University, Jisc, Janet or a third-party provider, the user must comply with that network's acceptable use requirements. Misuse of a partner or external network may also be treated as misuse of Bellmont College IT resources.

13. Social Media and Online Behaviour

Social media and public online platforms can support learning, employability, recruitment, student engagement and community building, but they also create risks relating to confidentiality, harassment, reputation, safeguarding, copyright, consumer protection and data protection. Users must act responsibly when their online activity is connected with Bellmont College, Liverpool Hope University, students, staff, partners or College business.

Users must:

- not publish confidential College, partner, student, staff or third-party information
- not present personal views as official Bellmont College or Liverpool Hope University statements
- not post content that is discriminatory, bullying, harassing, defamatory, threatening, obscene, extremist, hateful or otherwise harmful
- not share images, recordings, personal data or private communications without lawful basis and appropriate consent where required
- respect copyright and intellectual property when sharing images, teaching materials, extracts, videos, logos or third-party content
- follow the terms of service and community guidelines of each platform used
- avoid one-to-one personal social media relationships between staff and current students unless there is an approved educational, support or professional purpose and the arrangement is transparent and appropriate.

Concerns about online harassment, safeguarding, discrimination, sexual misconduct or student wellbeing must be escalated under the relevant route, including *(HSP1 Bellmont College Safeguarding and PREVENT Policy)*, *(SWP2 Bellmont College Equality, Diversity and Inclusion Policy)*, *(CAP3 Bellmont College Complaint and Appeal Policy and Procedure)* and *(QGP3 Bellmont College Student Handbook)*.

14. Data Protection, Confidentiality and Information Security

Users must handle personal data and confidential information carefully, lawfully and only for authorised purposes. Digital misuse can harm students, staff, partners and the College, and may create legal, regulatory, safeguarding, academic and reputational consequences.

Users must:

- access personal data only where they have a legitimate College, academic, support, governance or partnership need
- use College-approved systems for storing, sharing and processing College data
- avoid storing personal or sensitive College data on personal devices unless there is a clear authorised need and appropriate encryption or security control
- protect special category data, safeguarding information, disability information, complaints, appeals, assessment material, financial information and staff records with particular care
- use secure sharing methods and avoid unnecessary duplication of confidential data
- check recipients and access permissions before sharing files or links
- not transfer personal data outside approved locations or outside the UK unless authorised and supported by appropriate safeguards
- report any suspected or confirmed data breach, loss, misdirection, unauthorised disclosure or system compromise immediately to the Data Protection Officer and IT Service Desk
- follow retention, deletion, archiving and secure disposal requirements in *(BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy)*.

The College uses technical and organisational measures to protect information. These may include access controls, encryption, multi-factor authentication, backups, patching, antivirus protection, monitoring, audit logs, secure disposal, supplier due diligence, data protection impact assessments and user training.

Where data is held or processed by Liverpool Hope University as part of partnership arrangements, Bellmont College cooperates with the University and follows agreed data sharing, breach reporting and student support processes under *(LHU Liverpool Hope University Data Protection Policy)* and relevant partnership agreements.

15. Artificial Intelligence and Emerging Technologies

Artificial intelligence tools can support learning, productivity, accessibility, administration and creativity when used carefully. They can also create risks relating to personal data, confidentiality, copyright, academic integrity, bias, accuracy, transparency and over-reliance. Use of AI must be lawful, ethical and consistent with College and partner expectations.

Users must:

- use only College-approved AI tools for College business where approval is required
- not enter personal data, confidential information, assessment material, student records, staff records, safeguarding information, partner data or commercially sensitive information into public AI tools unless expressly approved and supported by appropriate safeguards
- check AI-generated content for accuracy, bias, plagiarism, accessibility, confidentiality and appropriateness before use

- declare or acknowledge AI use where required by academic, assessment, staff or publication rules
- not use AI tools to impersonate others, bypass assessment rules, fabricate evidence, produce misleading records, make automated decisions about students or staff without authorisation, or create harmful content
- ensure that any use of AI in teaching, assessment or student support is transparent, inclusive and consistent with *(LTP6 Bellmont College Academic Integrity and Misconduct Policy)*, and *(LHU Liverpool Hope University Generative AI Guidance)*.

Staff considering AI tools for administration, assessment, analytics, attendance, wellbeing, admissions or decision-making must consult the Head of IT, Data Protection Officer and Head of Quality and Operations before implementation. A data protection impact assessment and equality impact consideration may be required.

16. Software, Licensing, Copyright and Intellectual Property

Software and digital content must be acquired, installed, used and removed lawfully. Unapproved software can create licensing, cybersecurity, compatibility, accessibility, data protection and cost risks.

Users must:

- install, use or request software only through approved IT processes
- not copy, distribute, download, install or use unlicensed, pirated or unauthorised software
- not disable licence controls, digital rights management, update mechanisms or security settings
- comply with software licence terms, copyright law, database rights, Creative Commons licences and third-party terms of use
- not upload College or partner content to external platforms where doing so would breach copyright, confidentiality, data protection, contract terms or assessment security
- respect the intellectual property of students, staff, partners, publishers, software suppliers and external creators
- submit software requests to the IT Team for security, accessibility, data protection, procurement and licensing assessment.

The IT Team may remove unauthorised or unsupported software without notice where it creates risk, breaches licence terms or interferes with College operations.

17. Remote Working and Bring Your Own Device

Remote access and personal devices can support flexible working, blended learning and continuity of study, but they increase the need for secure behaviour. Users remain responsible for complying with this policy when away from College premises.

When working or studying remotely, users must:

- use approved remote access methods, VPNs, portals and cloud services
- keep home networks, routers and devices secure and updated
- ensure that screens, conversations and documents are not visible or accessible to unauthorised people
- not allow family members, friends, housemates or others to use College devices or accounts
- store paper records, portable devices and confidential information securely
- avoid using public Wi-Fi for sensitive work unless approved safeguards are used
- report loss, theft or compromise of a device immediately
- return College equipment on request, at the end of employment, at the end of study or when access is no longer authorised.

Users who connect personal devices to College or partner systems must:

- use devices that have up-to-date operating systems, security patches and anti-malware protection
- register devices with IT where required
- accept that access from personal devices may be restricted or withdrawn where security or data protection risk is identified
- not store College sensitive data on personal devices unless authorised and protected by appropriate security controls
- allow the College or partner to remove College data, restrict access or require remote wipe of College data where a device is lost, stolen, compromised, replaced, sold or no longer used for College purposes
- comply with *(HRP2 Bellmont College Employee Handbook)* and any relevant Liverpool Hope University device or wireless policy.

18. Digital Learning Systems, Assessment and LHU Resources

Digital learning systems are central to student experience. Bellmont College uses approved systems to support teaching, learning materials, assessment information, feedback, attendance, student support, communication and quality assurance. Where Liverpool Hope University systems are used, students and staff must follow University rules as well as this policy.

Students can expect:

- clear signposting to the digital systems they are expected to use
- reasonable support to access online learning resources, email, portals and assessment information
- reasonable adjustments or alternative formats where required and practicable
- communication about planned downtime, major disruption, system changes or access issues where these affect study
- proportionate contingency arrangements if a digital failure affects teaching, assessment submission, feedback, attendance recording or access to support.

Users must not use digital learning systems to upload harmful content, share assessment answers dishonestly, access another student's work, interfere with attendance or assessment records, breach academic integrity, harass others, distribute unauthorised recordings or undermine assessment security.

Where digital learning or assessment involves Liverpool Hope University systems, Bellmont College aligns local practice with applicable partner requirements and signposts users to *(LHU Liverpool Hope University IT Facilities Acceptable Use Policy)*, *(LHU Liverpool Hope University Information Security Policy)*, *(LHU Liverpool Hope University Student Guide to Regulations and Policies)* and *(LHU Liverpool Hope University Code of Student Conduct)*.

19. Accessibility, Inclusion, Safeguarding and Prevent

The College expects digital services and online behaviour to support an inclusive, respectful and safe learning and working environment. IT acceptable use therefore includes equality, accessibility, safeguarding and Prevent responsibilities.

Users must:

- not use IT resources to discriminate, harass, bully, victimise, abuse, exploit, intimidate, exclude or humiliate others
- respect reasonable adjustments, accessibility tools, assistive technologies and alternative communication needs
- not disable or interfere with accessibility features needed by another user
- use accessible formats and inclusive communication where materials are created for students or staff
- report safeguarding concerns, online exploitation, radicalisation concerns, harmful content, sexual misconduct, harassment or risk of harm promptly through the appropriate safeguarding route
- not access, download, store or distribute extremist or terrorist material except where authorised for a legitimate academic, safeguarding or investigative purpose and subject to approval and risk assessment
- follow *(SWP2 Bellmont College Equality, Diversity and Inclusion Policy)*, *(SWP1 Bellmont College Reasonable Adjustment and Special Considerations Policy)*, *(HSP1 Bellmont College Safeguarding and PREVENT Policy)*.

20. Monitoring, Privacy and Lawful Investigation

Bellmont College may monitor, log, review and investigate the use of IT resources for legitimate purposes. Monitoring helps maintain system performance, cybersecurity, safeguarding, academic integrity, business continuity, legal compliance, data protection, policy compliance and effective service delivery.

Monitoring may include:

- network, internet, Wi-Fi, VPN and firewall logs
- login, access, device and application logs

- email metadata and, where lawful and proportionate, email content
- file access, storage, sharing and deletion activity
- printing, copying and scanning activity
- security alerts, antivirus alerts, phishing reports and system audit trails
- use of virtual learning environments, online assessment tools, attendance systems and student portals
- use of College-managed devices, cloud services and collaboration platforms.

Monitoring and investigation is carried out only where there is a legitimate purpose and where it is lawful, necessary, proportionate and authorised. The College handles monitoring data in accordance with (BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy) and relevant privacy notices. Access to a user's account or content requires appropriate authorisation and may involve the Head of IT and Human Resources, Data Protection Officer, Chief Executive Officer, Safeguarding Team, Head of Quality and Operations or another senior officer depending on the nature of the concern.

Users should understand that College and partner IT resources are provided for College, academic and authorised purposes. Personal use may be limited and must not be assumed to be private where monitoring or investigation is required for a lawful and proportionate reason. Where Liverpool Hope University systems are involved, monitoring and investigation may also be governed by Liverpool Hope University policies and procedures.

21. Cybersecurity Incident Reporting and Business Continuity

Prompt reporting is essential. Many incidents can be contained quickly if users report them immediately. Users are not normally criticised for reporting a genuine mistake promptly, but deliberate concealment, delay or repeated careless behaviour may be treated seriously.

Users must immediately report the following to the IT Service Desk:

- suspected phishing, smishing, vishing or social engineering attempts
- loss, theft or compromise of a College or personal device used for College work or study
- suspected malware, ransomware, virus infection or unusual system behaviour
- accidental disclosure, loss, misdirection or unauthorised access to data
- unauthorised account access or suspicious login activity
- weaknesses, vulnerabilities, misconfigurations or exposed systems
- breach of this policy or any partner acceptable use policy
- system outage, disruption or digital access issue that affects teaching, assessment, student support or College operations.

If personal data may be involved, the user must also report the matter to the Data Protection Officer under *(BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy)*. If a safeguarding, Prevent, harassment, sexual misconduct or

risk-of-harm concern is involved, the user must also follow *(HSP1 Bellmont College Safeguarding and PREVENT Policy)* and the relevant reporting procedure.

The IT Team triages incidents, protects systems, preserves evidence where necessary, coordinates with internal and external stakeholders, communicates with affected users and supports continuity of teaching, assessment and services. Material incidents are escalated through the Senior Management Committee, Audit and Risk Committee and Board of Directors as appropriate, and through Liverpool Hope University partnership routes where partner systems or students are affected.

Contact: IT Service Desk - itsupport@bellmontcollege.co.uk | Tel: 020 3840 9294 | London.

22. Breaches, Restrictions and Disciplinary Action

A breach of this policy may place students, staff, College data, partner systems, learning continuity or the College's reputation at risk. Bellmont College responds fairly, proportionately and consistently, taking account of the nature of the breach, intent, impact, previous conduct, safeguarding considerations, legal duties and the need to protect others.

Possible responses include:

- advice, support, retraining or reminder of expectations
- temporary or permanent restriction, suspension or withdrawal of IT access
- removal of unauthorised software, files, devices or access permissions
- device quarantine, password reset, account lockout or remote wipe of College data
- formal investigation under the relevant staff, student, contractor or visitor process
- disciplinary action under *(HRP3 Bellmont College Staff Grievance and Disciplinary Policy)*, *(QGP3 Bellmont College Student Handbook)* or another applicable procedure
- academic misconduct action under *(LTP6 Bellmont College Academic Integrity and Misconduct Policy)* where the breach relates to assessment or academic integrity
- complaint, safeguarding, Prevent, harassment or wellbeing referral where appropriate
- termination of third-party access, contract review or supplier escalation
- notification to Liverpool Hope University where partner systems, students, data or academic arrangements are involved
- notification to the Information Commissioner's Office, Office for Students, law enforcement, insurers, awarding bodies or other external bodies where legally or contractually required.

The College may preserve system logs, access records, emails, files, device information and other evidence where this is necessary for investigation, legal

compliance, safeguarding, cybersecurity or disciplinary action. Evidence is handled confidentially and in accordance with data protection requirements.

23. Implementation, Training, Monitoring, Audit and Evidence

This policy is implemented through day-to-day operational controls, induction, staff training, student communication, access management, incident reporting, committee oversight, risk management and annual review. The implementation model is: identify the issue; assess the risk and impact; assign an owner; take corrective or preventive action; report to the relevant committee; escalate material risks; and close the action only when evidence shows it has been completed.

Implementation activity includes:

- publication of this policy to students, staff, directors and authorised third parties
- student induction and staff induction covering acceptable use, digital systems, passwords, data protection, safeguarding and incident reporting
- role-based training for staff with access to student records, sensitive data, finance systems, safeguarding records, assessment systems or partner systems
- periodic reminders on phishing, password security, AI use, data handling, copyright, social media and online conduct
- access reviews for staff, students, directors, contractors and system administrators
- IT security monitoring, patching, backups, vulnerability management and incident review
- website, portal and system accessibility checks where appropriate
- audit of compliance evidence, including access logs, training records, committee minutes, incident logs, risk registers, policy acknowledgements, data breach records, action plans and completion evidence
- review of student feedback, complaints, digital access issues and partner matters that may indicate weaknesses in IT provision or user understanding.

Training and evidence are monitored by the Head of IT, Data Protection Officer, Head of Quality and Operations, Senior Management Committee and relevant committees. Weaknesses are recorded, assigned to an owner and tracked until resolved.

24. Roles and Responsibilities

Role / body	Responsibilities
Board of Directors	Retains ultimate governance oversight of IT acceptable use as part of governance, risk, student protection, legal compliance and institutional accountability. Receives assurance on material incidents, cybersecurity risk, regulatory developments and policy review.

Role / body	Responsibilities
CEO	Holds executive accountability for ensuring that IT acceptable use, cybersecurity, data protection, student interests and partner obligations are resourced and implemented effectively.
Senior Management Committee	Leads operational implementation, prioritises resources, responds to material risks, receives incident reports and ensures that actions agreed by committees are completed.
Head of IT / IT Manager	Owns operational delivery of IT acceptable use controls, access management, system security, incident response, user support, monitoring, technical guidance, supplier engagement and policy maintenance.
Data Protection Officer	Advises on UK GDPR, data protection impact assessments, privacy notices, data breaches, data sharing, retention, training, monitoring and data protection compliance under *(BCP7 Bellmont College General Data Protection & Regulation (GDPR) Policy)*.
Head of Quality and Operations	Ensures that IT acceptable use supports academic quality, student experience, regulatory evidence, committee reporting and partnership expectations.
Academic Committee	Provides academic oversight where IT use affects teaching, learning, assessment, academic integrity, student outcomes, digital resources and partnership academic arrangements.
Head of Academic Programmes	Ensures that programme delivery, digital learning resources, assessment processes, academic support and online conduct are consistent with approved arrangements and student expectations.
Head of Professional Services	Ensures that admissions, registry, student support, finance, communications and operational services use systems securely and provide clear student-facing information.
Programme Coordinators and Module Tutors	Use digital systems responsibly, communicate expectations to students, protect assessment information, escalate access issues and support academic integrity.
Student Support and Safeguarding Staff	Use systems securely when handling support, wellbeing, safeguarding, disability, reasonable adjustment and confidential records, and escalate digital safeguarding concerns.

Role / body	Responsibilities
Managers and Line Managers	Ensure staff understand their responsibilities, complete training, follow access procedures and report changes in roles or leavers promptly to IT.
Students	Use IT resources lawfully, respectfully and for legitimate study purposes; protect accounts; follow assessment and academic integrity rules; report concerns promptly; and comply with this policy and applicable partner policies.
All Staff	Use IT resources professionally, protect personal data and confidential information, follow security controls, report incidents and support a respectful digital environment.
Directors and Committee Members	Use committee papers, email, collaboration tools and Bellmont College data securely, respecting confidentiality and data protection requirements.
Contractors, Consultants and Third Parties	Use only the access granted for the approved purpose, comply with this policy and contractual requirements, protect data and report incidents immediately.
Liverpool Hope University and Partner Representatives	Work with Bellmont College under agreed partnership routes where partner systems, students, data, academic arrangements or policies are affected.

25. Governance and Committee Oversight

IT acceptable use is monitored through Bellmont College governance and committee arrangements. The purpose of oversight is to ensure that digital risks, user conduct, incidents, student impacts and policy implementation are identified, evidenced, acted on and escalated. Committees should not only receive reports; they should test whether actions are effective and whether students, staff and partner obligations are protected.

Committee / body	How it implements this policy
Board of Directors	Approves the policy and receives assurance on material risks, cybersecurity, student protection, data protection, regulatory developments, partnership implications and significant incidents.
Audit and Risk Committee	Monitors cybersecurity, data protection, business continuity, legal compliance, audit findings, incident trends, supplier risks, access control and risk register entries.
Academic Committee	Provides academic oversight where IT affects teaching, learning, assessment, academic integrity, academic standards, quality, student outcomes or Liverpool Hope University partnership academic arrangements.

Committee / body	How it implements this policy
Senior Management Committee	Coordinates operational implementation, resources, urgent decisions, business continuity, partner escalation, cross-department action and review of material incidents.
Quality Committee	Receives assurance that IT acceptable use supports quality assurance, student experience, public information, complaints, appeals, policy implementation and regulatory evidence.
Learning and Teaching Committee	Reviews digital learning, online assessment, feedback systems, academic resources, module delivery, accessibility of learning resources and technology-related academic risks.
Recruitment, Admissions and Registry Committee	Monitors secure and accurate use of admissions, applicant communications, enrolment, attendance, engagement, student records and data integrity systems.
Student Staff Committee	Provides the student voice route for digital access concerns, online learning issues, assessment technology concerns, timetable or resource concerns and communication issues.
Safeguarding and Prevent Committee	Reviews digital safeguarding, Prevent, online harm, harassment, exploitation, radicalisation, harmful content and online reporting routes.
Equality, Diversity and Inclusion Committee	Monitors digital accessibility, inclusive communication, reasonable adjustments, online discrimination and equality impacts of systems or policy implementation.
IT and Data Protection Working Group	Coordinates operational activity between IT, data protection, quality, professional services and academic teams on incidents, controls, training, access and policy improvement.

26. Conclusion

Bellmont College is committed to maintaining a secure, lawful, inclusive and reliable digital environment that supports student success, staff effectiveness, academic quality, partnership delivery and public trust. Responsible IT use protects the College community, safeguards personal data, supports continuity of study, maintains academic integrity and helps students and staff work confidently in a digital learning environment.

This policy strengthens the existing Bellmont College IT acceptable use requirements by embedding them within a clear implementation and governance framework. It also reflects the current Liverpool Hope University partnership context and the College's future regulatory development. Bellmont College continues to review and improve its digital controls, student support, governance oversight and policy framework so that students' interests remain central as systems, risks and regulatory arrangements evolve.

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