“Enabling Students to Accomplish their Academic Goal”

General Data Protection and Regulation (GDPR) Policy

DOCUMENT CONTROL
Policy Number: BCP6
Version: 4.0
Date: March 2026
Owner: Head of Quality and Operations
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 personal data and handling information lawfully, fairly, transparently and securely. This policy explains how the College complies with the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and related data protection, privacy, information security and higher education regulatory expectations.

Bellmont College currently works with Liverpool Hope University as an awarding and academic partner for relevant higher education provision. Under this partnership, some student information, academic records, quality assurance records and regulatory information may be shared with Liverpool Hope University where this is necessary for admissions, enrolment, assessment, moderation, quality assurance, student support, student outcomes, awards, complaints, appeals or regulatory compliance. Bellmont College is also seeking Office for Students approval for its own funding arrangements. Future approval may affect processes, reporting routes, systems, responsibilities and data sharing arrangements, but Bellmont College continues to protect student interests, individual rights and information security during any transition.

This policy brings together the College's data protection principles, privacy practice, retention schedule, data breach response procedure, data subject rights procedure, data sharing and data processing requirements, DPIA register and data breach reporting form in one practical document. It is written for students, staff, directors, contractors, partners and third parties so that data protection is understood as part of everyday governance rather than a remote compliance exercise.

2. Purpose of the Policy

The purpose of this policy is to establish a clear and concise framework for the collection, use, storage, sharing, retention, disposal and protection of personal data processed by or on behalf of Bellmont College. It supports the College in demonstrating accountability and in maintaining confidence among students, staff, applicants, partners, regulators and the public.

The policy supports the College to:

- process personal data lawfully, fairly, transparently and securely;
- protect the privacy, dignity and rights of students, staff, applicants, visitors and other individuals;
- maintain accurate student, staff, academic, finance, safeguarding, complaints, appeals and governance records;
- provide clear privacy information and respond properly to data subject rights requests;
- manage data sharing and third-party processing through appropriate controls;
- respond quickly and proportionately to actual or suspected personal data breaches;
- retain information only for as long as it is needed and dispose of it securely;
- embed data protection in quality assurance, student protection, information governance, business continuity and committee oversight.

This policy should be read alongside the College's wider information and governance documents, including the *(QGP6 Bellmont College Information Governance, Public Information and Transparency Policy)*, the *(BCP6 Bellmont College Information Security and Cybersecurity*

Policy), the *(BCP8 Bellmont College IT Acceptable Use Policy)*, the *(QGP1 Bellmont College Quality Handbook)*, the *(Bellmont College Safeguarding and PREVENT policy)*, the *(CAP1 Bellmont College Student Protection Plan and Policy)* and the *(CAP3 Bellmont College Complaint and Appeal Policy and Procedure)*.

3. Scope of the Policy

This policy applies to all personal data processed by Bellmont College or on its behalf, whether held electronically, on paper, in cloud systems, email, learning platforms, student record systems, finance systems, CCTV, audio or video recordings, committee papers or archived records.

It applies to:

- current, former and prospective students;
- current, former and prospective staff, directors, contractors, consultants and volunteers;
- applicants, enquirers, alumni, visitors, suppliers, placement providers, complainants and correspondents;
- Liverpool Hope University and any future awarding, validating, collaborative, franchising, funding or regulatory partner where personal data is shared lawfully;
- all staff and third parties who collect, access, store, disclose, analyse, transfer, archive or destroy personal data for College purposes.

The policy applies across the full student and staff journey, including enquiry, admissions, enrolment, induction, teaching, attendance, assessment, student support, safeguarding, complaints, appeals, disciplinary matters, graduation, employment, finance, quality assurance, regulatory reporting, audit, research and alumni activity.

4. Regulatory, Legal and Quality Assurance Framework

Requirement	Relevance to this Policy
UK GDPR and Data Protection Act 2018	Set the data protection principles, lawful bases, special category rules, rights, records of processing, DPIAs, breach notification and accountability duties.
Privacy and Electronic Communications Regulations 2003	Apply to direct marketing, cookies and electronic communications.
Human Rights Act 1998	Supports respect for private and family life when personal data is handled.

Computer Misuse Act 1990	Supports controls against unauthorised access and system misuse.
Freedom of Information Act 2000 and Environmental Information Regulations 2004	Inform transparency and records handling where applicable.
Equality Act 2010	Requires fair, accessible and non-discriminatory data handling and communication.
Safeguarding and Prevent duties	Support lawful and proportionate information sharing where protection of students or others is necessary.
Higher Education and Research Act 2017 and OfS regulatory framework	Provide the higher education regulatory context for information, governance and reporting.
Office for Students conditions B, C, E and F where relevant	Inform quality, standards, student protection, consumer protection, governance, accountability and reporting controls.
Competition and Markets Authority expectations	Support accurate information, fair treatment, fair terms and accessible redress.
UK Quality Code for Higher Education	Supports reliable information, evidence-based governance, academic standards, quality and partnership working.
Office of the Independent Adjudicator Good Practice Framework	Relevant where complaints, appeals or student records are involved.
HESA / Jisc, Student Loans Company, UKVI, HMRC and other reporting requirements	Apply where data is used for statutory, funding or regulatory reporting.
Liverpool Hope University partnership requirements	Apply where students are studying under Liverpool Hope University arrangements and

	data is shared for academic, quality or support purposes.

5. Key Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person, such as name, student number, contact details, online identifiers, images, academic records, attendance, support information or financial records.
Special category data	More sensitive personal data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health information, sex life or sexual orientation.
Criminal offence data	Information relating to criminal convictions, offences, allegations, DBS checks or safeguarding disclosures. It requires particular legal safeguards.
Processing	Any operation performed on personal data, including collection, recording, storage, use, sharing, consultation, alteration, restriction, erasure, archiving or destruction.
Data controller	The organisation that determines why and how personal data is processed. Bellmont College is a controller for personal data processed for its institutional purposes.
Data processor	A person or organisation processing personal data on behalf of the College, such as a cloud service provider, payroll provider or student system provider.
Data subject	The living individual to whom personal data relates.
Data Protection Officer	The designated person who advises on data protection obligations, monitors compliance, supports staff, handles rights requests and breach management, and acts as a contact point with the ICO.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
DPIA	A Data Protection Impact Assessment used to identify and reduce privacy risks before high-risk processing begins.

6. Core Data Protection Principles

Bellmont College applies the UK GDPR principles to all personal data. These principles are practical standards for good information management and are embedded through procedures, systems, committee oversight and staff training.

Principle	Bellmont College commitment
Lawfulness, fairness and transparency	Bellmont College uses personal data only where there is a lawful basis, will treat individuals fairly and will explain how information is used through privacy notices and clear communications.
Purpose limitation	Personal data will be collected for specified, explicit and legitimate purposes and will not be used in ways that are incompatible with those purposes unless a lawful basis permits this.

Data minimisation	The College will collect and use only the personal data needed for the relevant academic, support, employment, finance, safeguarding, legal or regulatory purpose.
Accuracy	Records must be accurate and kept up to date where necessary. Students and staff are expected to tell the College promptly when their personal details change.
Storage limitation	Personal data will not be retained for longer than necessary and will be managed in line with the Data Retention Schedule in this policy.
Integrity and confidentiality	Personal data must be protected against unauthorised access, loss, destruction, alteration or disclosure through appropriate technical and organisational measures.
Accountability	The College must be able to demonstrate compliance through policies, procedures, training, records, DPIAs, contracts, breach logs, audit trails and committee reporting.

7. Lawful Bases for Processing

The College will identify a lawful basis before processing personal data. In higher education, more than one lawful basis may apply depending on the purpose. The lawful basis must be recorded in the Record of Processing Activities and reflected in privacy notices.

Lawful basis	Typical use
Contract	Used where processing is necessary for a student contract, staff contract, supplier contract or steps before entering into a contract.
Legal obligation	Used where the College must comply with legislation or statutory reporting, such as HMRC, UKVI, safeguarding, employment, health and safety or regulatory requirements.
Public task	Used where processing is necessary for education, quality assurance, regulatory reporting or other tasks carried out in the public interest.
Legitimate interests	Used where the College or a third party has a legitimate interest, provided this does not override individual rights and freedoms.
Vital interests	Used where processing is necessary to protect someone's life or serious health and safety interests.
Consent	Used only where consent is appropriate, freely given, specific, informed and capable of being withdrawn without unfair disadvantage.

Special category data and criminal offence data require additional safeguards. Bellmont College processes such data only where a UK GDPR Article 9 condition or Data Protection Act 2018 Schedule 1 condition applies, and where processing is necessary, proportionate and properly protected. Examples include disability support, safeguarding, wellbeing support, equality monitoring, DBS checks and serious incident management.

8. Student Personal Data, Regulatory Disclosure and Partnership Arrangements

Bellmont College processes student personal data to deliver and administer higher education. This includes enquiry and application records, admissions decisions, enrolment, attendance,

engagement, assessment, progression, achievement, academic support, wellbeing, disability support, safeguarding, finance, complaints, appeals, disciplinary matters, learning analytics, student feedback and regulatory reporting.

Student data may be used for teaching and learning, assessment, student support, safeguarding, reasonable adjustments, quality assurance, external examination, programme monitoring, academic standards, continuation and completion analysis, equality monitoring, student protection and institutional planning. Bellmont College ensures that such use is lawful, proportionate and clearly explained.

Where students are studying under Liverpool Hope University arrangements, Bellmont College may share necessary student information with Liverpool Hope University for academic administration, moderation, external examining, awarding qualifications, student support, quality assurance, complaints, appeals, student records, regulatory reporting and partnership oversight. Bellmont College maintains appropriate data sharing controls and will explain the division of responsibilities to students where relevant.

The College may also share personal data where lawful and necessary with bodies such as the Office for Students, HESA / Jisc, Student Loans Company, UKVI, HMRC, local authorities, professional bodies, external examiners, placement providers, auditors, insurers, legal advisers, emergency services, safeguarding authorities, IT providers, learning platform providers, plagiarism detection services and survey providers. Data will not normally be shared with parents, guardians, spouses, partners or next of kin without the student's consent, unless legal, safeguarding, vital interests or serious welfare reasons justify disclosure.

9. Privacy Notices, Transparency and Communication

Bellmont College provides clear privacy information at or before the point personal data is collected, unless an exemption applies. Privacy notices will explain who the College is, why personal data is used, the lawful basis, what data is collected, who it may be shared with, retention periods, international transfers where relevant, rights of individuals and how to complain.

Privacy information must be accessible and written in plain language. Where students or staff need alternative formats or support to understand information, the College will make reasonable adjustments in line with the *(SWP2 Bellmont College Equality, Diversity and Inclusion Policy)* and the *(SWP1 Bellmont College Reasonable Adjustment and Special Considerations Policy)*.

Transparency also applies to student-facing public information. Information about data use, course administration, partner responsibilities, complaints, appeals, learning platforms and student support must be consistent with the *(QGP6 Bellmont College Information Governance, Public Information and Transparency Policy)* and should not mislead students or applicants about how their information will be used.

10. Data Subject Rights Procedure

Individuals have rights under UK GDPR. Bellmont College handles all rights requests fairly, securely and within statutory timescales. Requests do not need to mention UK GDPR to be

valid and may be made verbally or in writing. Staff must forward any possible rights request to the Data Protection Officer promptly.

Right	How Bellmont College responds
Right to be informed	Individuals must receive clear information about how their personal data is used.
Right of access	Individuals may request copies of their personal data. This is commonly known as a Subject Access Request.
Right to rectification	Individuals may ask for inaccurate data to be corrected or incomplete data completed.
Right to erasure	Individuals may ask for deletion in certain circumstances, subject to legal, academic, regulatory, safeguarding and contractual requirements.
Right to restrict processing	Individuals may ask for processing to be restricted in certain circumstances.
Right to data portability	Individuals may request transfer of certain data provided by them where processing is based on consent or contract and automated processing applies.
Right to object	Individuals may object to certain processing, including direct marketing and some processing based on public task or legitimate interests.
Automated decision-making rights	Individuals have rights relating to solely automated decisions that produce legal or similarly significant effects. The College does not normally make such decisions without human involvement.

10.1 Procedure for rights requests

1. Requests must be sent to, or immediately forwarded to, the Data Protection Officer. Staff must not ignore, delay or informally handle requests without advice.
2. The Data Protection Officer will log the request, verify identity where necessary, clarify the request if it is unclear and identify the relevant departments or systems.
3. The College will normally respond within one calendar month. Where a request is complex or multiple requests have been made, the period may be extended by up to two further months, and the individual will be informed.
4. Information will be reviewed for third-party personal data, confidentiality, safeguarding, legal privilege, regulatory restrictions, academic integrity, assessment confidentiality and any exemptions that may apply.
5. Responses will be provided securely and in an accessible format wherever reasonably possible.
6. A record of the request, decision, response, exemptions considered and date of closure will be retained for audit purposes.

11. Consent, Direct Marketing and Automated Decision-Making

Consent will be used only where it is the most appropriate lawful basis. Consent must be freely given, specific, informed and unambiguous. It must be recorded and capable of withdrawal as easily as it was given. The College will not rely on consent where an individual has no real

choice, where processing is required by law or contract, or where a different lawful basis is more appropriate.

Direct marketing and electronic communications will comply with UK GDPR and the Privacy and Electronic Communications Regulations 2003. Marketing preferences and opt-out requests must be respected promptly. Bellmont College maintains evidence of consent or other lawful marketing basis where required.

The College does not normally make decisions about students or staff based solely on automated processing that produces legal or similarly significant effects. If such processing is proposed, a Data Protection Impact Assessment must be completed and appropriate safeguards must be approved before implementation.

12. Data Sharing, Third Parties and International Transfers

The College may share personal data with third parties where it is lawful, necessary, proportionate and secure. Data sharing must be limited to what is needed for the purpose and must be supported by a suitable agreement where regular, significant or sensitive sharing takes place.

Before sharing personal data, staff must consider whether:

- there is a clear purpose and lawful basis;
- the data is accurate, relevant and limited to what is necessary;
- the recipient is authorised and has appropriate security arrangements;
- a Data Sharing Agreement or Data Processing Agreement is required;
- students or staff have been informed through a privacy notice unless an exemption applies;
- special category or criminal offence data requires additional safeguards;
- international transfer safeguards are required.

Personal data must not be transferred outside the United Kingdom unless there is an adequacy regulation, appropriate safeguards such as UK-approved standard contractual clauses, an approved derogation or explicit legal advice confirming the transfer route. International transfers must be recorded and reviewed by the Data Protection Officer.

13. Data Processing Agreement Requirements

A Data Processing Agreement is required where a third party processes personal data on behalf of Bellmont College. This includes suppliers such as cloud services, student record systems, learning platforms, payroll providers, online assessment services, survey systems, IT support providers and other service providers acting on College instructions.

The agreement must be in writing and must include the Article 28 UK GDPR requirements. The following checklist will be used before the processor starts work.

DPA requirement	What must be included
Parties and status	Identify Bellmont College as controller where applicable and the supplier as processor, unless another lawful status applies.

Subject matter and duration	Describe the service, processing activity, start date, duration and end/termination arrangements.
Nature and purpose	Explain what the processor will do with the data and why.
Types of data and data subjects	List categories of personal data and individuals affected, including any special category or criminal offence data.
Documented instructions	Require processing only on documented instructions from the College.
Confidentiality	Require staff and sub-processors to be bound by confidentiality.
Security measures	Set out technical and organisational measures, including access control, encryption where appropriate, backups, incident response and secure disposal.
Sub-processing	Require prior authorisation for sub-processors and equivalent contractual obligations.
Data subject rights	Require assistance with rights requests.
Breaches	Require prompt notification of actual or suspected personal data breaches and assistance with investigation and notification.
DPIAs and audits	Require assistance with DPIAs, audits, inspections and evidence requests.
Return or deletion	Require return or secure deletion of personal data at the end of the service unless law requires retention.

14. Data Sharing Agreement Requirements

A Data Sharing Agreement is required where Bellmont College and another organisation share personal data as controllers, or where regular data sharing involves significant, sensitive or repeated transfers. This may include sharing with Liverpool Hope University, awarding bodies, placement providers, professional bodies, local authorities or other education partners.

The agreement should be proportionate to the risk and should include the following core information.

DSA requirement	What must be included
Purpose	The reason for sharing and the expected benefit or legal requirement.
Parties and contacts	The organisations involved, controller/processor status and nominated data protection contacts.
Data categories	The information to be shared, including whether special category or criminal offence data is included.
Data subjects	The individuals whose data will be shared.
Lawful basis and conditions	The Article 6 lawful basis and any Article 9 or Data Protection Act 2018 conditions.
Fair processing	How individuals will be informed, or why an exemption applies.
Security and transfer method	How the data will be protected, transferred, accessed and stored.
Retention and disposal	How long each party keeps the data and how it is deleted or archived.

Rights requests	How parties coordinate access, correction, objection, restriction or deletion requests.
Breach management	How incidents are reported, investigated, escalated and notified.
Review and termination	Review date, change control, end of sharing and records to be retained.

15. Data Security, Confidentiality and Information Governance

Data protection depends on secure systems, careful behaviour and good information governance. Bellmont College applies appropriate technical and organisational controls to protect personal data from accidental or unlawful loss, destruction, alteration, unauthorised disclosure or access.

Controls include role-based access, password protection, multi-factor authentication where available, secure storage, encryption where appropriate, backups, secure disposal, access reviews, staff training, incident reporting, system monitoring, third-party due diligence, physical security, clear desk and clear screen practice, and secure communication methods.

Staff working remotely or using mobile devices must access personal data only through approved systems and must not store College records on personal devices, unapproved cloud services, social media, personal messaging applications or insecure channels. Staff must follow the *(BCP8 Bellmont College IT Acceptable Use Policy)*, the *(BCP6 Bellmont College Information Security and Cybersecurity Policy)*, the *(HRP2 Bellmont College Employee Handbook)* and the *(QGP6 Bellmont College Information Governance, Public Information and Transparency Policy)*.

16. Data Retention Schedule

Personal data must not be kept for longer than necessary. The following schedule sets out Bellmont College's standard retention periods. Longer retention may be required where there is an active complaint, appeal, investigation, safeguarding concern, legal claim, audit, regulatory request, partnership requirement or statutory duty. Shorter retention may apply where the purpose has ended and no lawful reason remains to keep the data.

Record type	Retention period	Reason / notes
Student summary record	Permanent	To evidence attendance, award, outcome, progression and verification of study.
Detailed student file, including admissions, enrolment, learning support, progression and withdrawal records	6 years after completion or withdrawal	Supports academic administration, complaints, appeals, regulatory evidence and limitation periods.
Assessment marks, moderation records, boards, external examiner evidence and award decisions	6 years after award or withdrawal; award summary permanent	Academic standards, quality assurance and regulatory evidence.

Assessment scripts, submitted work and feedback records	Normally 1 academic year after final decision, unless needed for complaint, appeal, quality review or partner requirement	Supports assessment integrity and review while avoiding unnecessary retention.
Attendance, engagement and submission records	6 years after completion or withdrawal	Supports student support, funding, compliance, audit and regulatory evidence.
Student complaints, academic appeals and disciplinary records	6 years after case closure; serious cases may be retained longer on advice	Supports fairness, legal defence, regulatory review and trend monitoring.
Safeguarding, Prevent, serious welfare and risk records	Retain in line with safeguarding need; normally up to 25 years after last contact for serious safeguarding records, subject to review	Protects vulnerable individuals and supports legal and safeguarding duties.
Reasonable adjustments, disability, wellbeing and special considerations records	6 years after completion or withdrawal, unless safeguarding or legal reasons require longer	Supports inclusive provision and evidence of decisions.
Applicant records - unsuccessful applicants	6 months after admissions cycle, unless complaint, appeal or legal reason requires longer	Supports admissions fairness and equality monitoring.
Staff personnel and employment records	6 years after end of employment; pension or statutory records may be longer	Employment, HMRC, pension, legal and audit purposes.
Recruitment records - unsuccessful staff applicants	6 months after recruitment exercise	Equality monitoring and recruitment challenge period.
DBS and right-to-work evidence	Record of check retained; certificates not copied unless lawful and necessary. Right-to-work records 2 years after employment ends	Legal compliance, safeguarding and audit.
Financial, payroll, invoices, payment and tax records	7 years after financial year end	HMRC, audit, financial control and funding evidence.
Supplier due diligence, contracts, Data Processing Agreements and Data Sharing Agreements	6 years after contract or sharing arrangement ends, unless legal or regulatory reason requires longer	Contract management, audit and accountability.
CCTV (if applicable)	Normally up to 30 days unless needed for investigation, safeguarding, insurance or legal purposes	Security, incident investigation and safeguarding.
Data subject rights request records	3 years after closure	Evidence of compliance and decision-making.

Data breach records and breach reporting forms	6 years after closure; serious breaches may be retained longer on advice	Accountability, audit and ICO evidence.
DPIAs, Records of Processing Activities and risk assessments	Life of processing activity plus 6 years	Accountability and evidence of data protection by design.
Research data involving personal data	As required by ethics approval, funder rules or participant information; normally anonymise as soon as possible	Research integrity, funder compliance and participant rights.
Committee papers containing personal data	According to committee record schedule; confidential case papers retained only as long as needed	Governance evidence and confidentiality.

At the end of the retention period, records must be securely destroyed, anonymised or archived where a lawful basis applies. Paper records must be securely shredded or placed in approved confidential waste. Electronic records must be securely deleted, anonymised or archived in accordance with IT and information security procedures.

17. Data Protection Impact Assessments and DPIA Register

A Data Protection Impact Assessment must be completed before starting processing that is likely to result in a high risk to individuals. This includes new systems, high-risk student monitoring, large-scale special category data, safeguarding or wellbeing systems, automated decision-making, new surveillance, large-scale sharing, new technologies, or significant changes to existing processing.

The Data Protection Officer must be consulted during the DPIA. If risks cannot be reduced to an acceptable level, the College must consider whether processing should proceed and whether consultation with the ICO is required.

17.1 DPIA Register

The Data Protection Officer will maintain a DPIA Register. The register may be held electronically and must be available for audit and committee assurance.

DPIA Register field	Entry / status
DPIA reference	
Project / processing activity	
Department / owner	
Purpose of processing	
Data subjects and data categories	
Special category / criminal offence data?	
Lawful basis and Article 9 condition	
Risk level before controls	
Key risks identified	

Mitigating controls and actions	
Residual risk rating	
DPO advice	
Approval decision and date	
Review date	

18. Data Breach Response Procedure

All actual or suspected personal data breaches must be reported immediately to the Data Protection Officer. Early reporting is essential because the College may need to notify the ICO within 72 hours of becoming aware of a notifiable breach. Staff must not attempt to conceal, delay, delete or resolve a breach without reporting it.

Procedure step	Required action
1. Identify and report	Any staff member, student, contractor or partner who becomes aware of an actual or suspected breach must report it immediately using the Data Breach Reporting Form or by contacting the Data Protection Officer directly. Urgent cyber incidents must also be reported to the IT and Information Security Lead.
2.Contain and preserve evidence	The relevant team must take immediate steps to reduce harm, such as recalling an email, disabling access, isolating a device, retrieving documents, changing passwords or preserving audit logs. Evidence must not be destroyed.
3. Log and triage	The Data Protection Officer will open a breach record, assess urgency, identify affected data and individuals, and coordinate with IT, Registry, Student Support, Safeguarding, HR, Finance, the relevant manager and Liverpool Hope University where partnership data is involved.
4. Risk assessment	The Data Protection Officer will assess the likelihood and severity of risk to individuals, including identity theft, financial loss, distress, discrimination, confidentiality breach, safeguarding risk, academic disadvantage or loss of control over data.
5. Notification decision	Where the breach is likely to result in a risk to rights and freedoms, the College will notify the ICO without undue delay and, where feasible, within 72 hours. Where the breach is likely to result in a high risk, affected individuals will also be informed without undue delay.
6. Investigation and remediation	The College will investigate the root cause, implement corrective action, support affected individuals, recover data where possible and review whether policy, training, access controls or supplier arrangements require change.
7. Governance reporting and closure	Significant breaches will be reported to the Senior Management Team and Board of Directors. All breaches, including non-notifiable incidents, will be recorded and closed only when actions have been completed and evidence retained.

19. Data Breach Reporting Form (GDPR - Higher Education)

This form should be completed as soon as possible for any actual or suspected personal data breach. Do not delay reporting because all information is not yet available. The Data Protection Officer will update the record as more details become known.

Form field	Details
Date and time discovered	
Reported by / role / contact details	
Department or service area	
Date and time breach occurred, if known	
Type of breach	Loss / theft / unauthorised disclosure / cyber incident / email error / incorrect record / system access / paper record / other
Description of what happened	
Systems, files, emails or records involved	
Categories of individuals affected	Students / applicants / staff / alumni / contractors / visitors / research participants / other
Approximate number of individuals affected	
Categories of personal data involved	
Special category or criminal offence data involved?	Yes / No / Unsure
Immediate containment actions taken	
Who has the data now?	
Likely consequences for individuals	
Is Liverpool Hope University or another partner involved?	Yes / No / Unsure
Has IT or Information Security been notified?	Yes / No / Not applicable
Has Safeguarding or Student Support been notified?	Yes / No / Not applicable
DPO risk assessment	
ICO notification required?	Yes / No / Under review
Affected individuals notification required?	Yes / No / Under review
Corrective actions and owner	
Date closed and closure approved by	

20. Records of Processing Activities, Research Data and Specialist Records

Bellmont College maintains Records of Processing Activities describing what personal data is processed, why it is processed, lawful bases, data subjects, data categories, recipients, transfers, retention periods and security measures. Departments must provide accurate information to the Data Protection Officer and notify changes promptly.

Research involving personal data must comply with UK GDPR, the Data Protection Act 2018, ethical approval requirements, participant information and any funder conditions. Research data should be anonymised or pseudonymised where possible. A DPIA must be completed where research involves high-risk processing.

Specialist records such as safeguarding, PREVENT, wellbeing, disability support, complaints, appeals, misconduct and financial hardship records must be handled with additional care. Access must be limited to staff with a genuine need to know, and sharing must be lawful, proportionate and documented. Relevant teams must follow the *(Bellmont College Safeguarding Framework)*, the *(SWP4 Bellmont College Mental Health and Wellbeing Policy)*, the *(SWP2 Bellmont College Equality, Diversity and Inclusion Policy)*, the *(CAP5 Bellmont College Academic Appeals Policy)* and the *(CAP3 Bellmont College Complaint and Appeal Policy and Procedure)*.

21. Complaints, ICO Contact and Enforcement

Individuals who are concerned about how their personal data has been handled should contact the Data Protection Officer in the first instance. The College will investigate data protection concerns fairly, confidentially and promptly. Students may also raise issues through the relevant complaints route where the matter relates to their student experience.

Individuals have the right to complain to the Information Commissioner's Office if they believe their data protection rights have not been respected. ICO contact details are: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; telephone 0303 123 1113; website www.ico.org.uk.

Failure by staff to comply with this policy may result in management action, removal of system access, disciplinary action, referral to professional or regulatory bodies, contract termination or legal action. Students who misuse personal data may be subject to the *(QGP4 Bellmont College Student Handbook)*. Contractors, consultants, suppliers and processors may be subject to contractual remedies, audit action or termination.

22. Implementation Framework

This policy is implemented through everyday systems, staff responsibilities, student-facing communications, committee reporting, risk management, audit evidence and annual review. Data protection is not a single annual compliance task. It must be considered whenever the College collects information, introduces a system, changes a process, shares data, responds to a concern or makes a decision affecting students or staff.

The implementation model is: identify the processing activity; confirm the lawful basis; inform individuals; minimise data; apply security controls; assess risk; put agreements in place where needed; retain records only as long as necessary; report incidents; monitor evidence; review and improve.

Activity	Implementation route
New or changed processing	Complete a processing review and, where needed, a DPIA before the activity begins.
Student data sharing with Liverpool Hope University or other partners	Confirm purpose, lawful basis, minimum data, secure transfer and DSA/DPA requirements.
Third-party supplier processing	Complete due diligence and ensure Article 28 DPA clauses are in place before data is shared.
Data subject rights request	Forward to DPO, log, verify, gather data, review exemptions and respond within timescale.
Personal data breach	Report immediately, contain, assess, notify if required, remediate and close actions.
Retention and disposal	Apply the schedule, securely destroy or archive, and record high-risk disposal where needed.
Training and awareness	Provide induction, annual refresher and targeted training for high-risk roles.

23. Roles and Responsibilities

Role / body	Responsibilities
Board of Directors	Retains ultimate governance oversight for data protection, information governance, risk assurance, institutional sustainability and regulatory compliance.
CEO	Holds executive accountability for effective implementation, resourcing, escalation and protection of students, staff and institutional information.
Data Protection Officer	Advises on UK GDPR and Data Protection Act 2018 obligations, monitors compliance, manages rights requests and breach response, maintains the ROPA, DPIA Register and breach records, provides training advice and acts as the contact point with the ICO.
Head of Quality and Operations	Coordinates policy implementation, quality assurance, regulatory monitoring, committee reporting, risk monitoring, public information review, partnership liaison and evidence gathering.

Head of Academic Programmes	Ensures that academic delivery, assessment records, module activity, attendance, engagement, student outcomes and academic data are accurate, secure and appropriately escalated where risks arise.
Head of Professional Services	Ensures that admissions, registry, student support, finance communications, applicant information, enrolment processes and operational services support accurate records, fair treatment, confidentiality and compliance.
Head of IT	Maintains system access controls, cybersecurity incident coordination, audit logs, secure evidence preservation, system recovery and technical support where data protection concerns involve digital systems.
Finance Lead or designated finance personnel	Ensure finance, payroll, supplier, payment, funding and procurement records are accurate, protected, retained and shared only where lawful and necessary.
Safeguarding Team and Student Support staff	Handle wellbeing, safeguarding, disability, reasonable adjustment, hardship and vulnerability information lawfully, proportionately and confidentially, and escalate concerns where data sharing is necessary to protect students or others.
Programme Coordinators and Module Tutors	Maintain accurate teaching, attendance, engagement, assessment and feedback records, support students appropriately, and escalate data accuracy, confidentiality, academic integrity or student support concerns.
All staff	Act honestly, complete training, follow controls, keep accurate records, protect Bellmont College information, report breaches promptly, seek advice when unsure and cooperate with audits or investigations.
Students	Provide truthful and up-to-date information, use Bellmont College systems responsibly, protect accounts and personal data, report suspicious requests or data concerns, and cooperate with reasonable checks.
Contractors, consultants, suppliers and partners	Comply with contractual, data protection, confidentiality, security, audit and breach reporting requirements and process personal data only as authorised.

24. Governance and Committee Oversight

Bellmont College monitors implementation through its committee and governance structure. This ensures that data protection is linked to academic quality, student protection, risk management, information governance, safeguarding, equality, digital continuity and partnership oversight.

Committee / body	How it implements this policy
Board of Directors	Receives assurance on compliance, significant breaches, data protection risks, regulatory developments, audit findings and material partnership or funding changes.
Audit and Risk Committee	Advises the Board of Directors on audit, internal control, risk management, regulatory compliance and assurance where data protection or cybersecurity matters identify wider institutional risk.
Academic Committee	Maintains academic oversight where data protection risks affect academic standards, student outcomes, assessment records, quality assurance or partner responsibilities.
Senior Management Committee	Coordinates operational implementation, resourcing, incident response, transition planning, partner liaison and corrective actions.
Quality Committee	Provides central assurance on policy implementation, quality records, student outcomes data, complaints and appeals trends, public information and compliance evidence.
Learning and Teaching Committee	Reviews academic data integrity, assessment records, learning analytics, student engagement systems and academic process risks.
Recruitment, Admissions and Registry Committee	Monitors applicant and student records, admissions data, enrolment, attendance, engagement, regulatory reporting and records accuracy.
Student Staff Committee and Partnership Routes	Provides a student voice route for data or system issues affecting students. Liverpool Hope University partnership matters are escalated through the relevant operational, academic and strategic partner routes where applicable.

25. Training, Monitoring, Audit and Evidence

All staff will receive data protection training at induction and periodic refresher training. Staff in higher-risk roles, including admissions, registry, student support, safeguarding, HR, finance, IT, quality assurance and academic administration, will receive additional role-specific guidance where required.

Monitoring will include policy review, breach analysis, data subject rights logs, DPIA review, ROPA review, retention checks, supplier due diligence, data sharing agreement review, privacy notice review, information security checks, staff training records, committee reporting, complaints analysis, audit findings and regulatory updates.

Evidence retained may include training records, committee minutes, breach forms, breach registers, DPIAs, ROPA entries, retention reviews, disposal records, privacy notices, contracts, Data Processing Agreements, Data Sharing Agreements, audit reports, action logs, system access reviews, data quality checks and advice from the Data Protection Officer.

26. Contact Details

Data Protection Officer (DPO)

Email: dpo@bellmontcollege.co.uk

Address: Bellmont College 1st Floor 9 Lymington Avenue Wood Green London N22 6EA

ICO Website: https://www.ico.org.uk

27. Conclusion

Bellmont College recognises that data protection is essential to trust, student protection, academic quality, safeguarding, regulatory compliance and institutional accountability. Bellmont College handles personal data responsibly and ensures that staff, students, directors, partners and processors understand their responsibilities.

As Bellmont College continues to work with Liverpool Hope University and progresses towards its own OfS funding arrangements, it maintains clear, lawful and secure information governance arrangements. Future changes to systems, reporting or partnership processes are managed carefully so that individual rights, student interests and regulatory expectations remain protected.

Bellmont College General Data Protection & Regulation (GDPR) Policy					
Version	**Date**	**Author(s)**	**Amendments**	**Approved by**	**Next review**
1	March 2023	Head of Quality and Operations	New document	Board of Directors	February 2024
2	February 2024	Head of Quality and Operations	Reviewed; no substantive update recorded	Board of Directors	October 2024
3	October 2024	Head of Quality and Operations	Revised document	Board of Directors	October 2025
4	March 2026	Head of Quality and Operations	Revised document	CEO / Board of Directors	March 2027