BORDERS COLLEGE

Data Protection Policy

February 2025

History of Changes

Version	Description of Change	Authored by	Date
Version	Description of Change	Authored by	Date
1.1	Information provided on where further guidance on data protection issues can be found. Direct marketing and CCTV surveillance added to the scope.	D Killean	16 May 2016
2.0	Fully updated to comply with GDPR and the new DPA. Covers the principles of the law and the rights of data subjects and what this means for the college. Some parts of the policy (e.g. marketing) have been removed and a separate procedure will be developed focusing on DPA and marketing. This is also the case for CCTV.	A Wilson	28 August 2018
2.1	Updated for readability Updated to include special category data requirement and reference to DP Champions Added Annex D relating to special category and criminal offence data Added DP Assurance Framework Amended re BREXIT	H Robertson/ A Wilson/L Bird	17 December 2021
2.2	Moved to new Policy Template. Amendments made for brevity and clarity.	K Robb / L Bird	February 2025

1.0 Introduction

1.1 Information, and how it is processed is of vital importance to the efficient functioning of Borders College.

1.2 This policy sets out the legal framework which governs the college's use of personal data, its commitment to protecting personal data and the obligations in relation to data handling. The college will meet the requirements of data protection legislation, including the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), associated guidance and applicable codes of practice. **Annex A** provides definitions from data protection law.

1.3 Annex D is the College's Policy Document relating to the processing of Special Category Data.

1.4 This policy should be read in conjunction with the Electronic Systems Policy and Procedure, the Information Security Policy and Data Protection guidance documents.

1.5 Any questions or concerns about compliance with this policy, must be reported to gdpr@borderscollege.ac.uk.

2.0 Scope

2.1 This policy applies to:

- all data created or received in the course of college business, in all formats:
- personal and special category data; confidential and commercially sensitive data
- data held or transmitted in physical (including paper) and electronic formats.
- data transmitted in verbal format (in conversation, in a meeting, or over the telephone).

2.2 The policy applies to and must be followed by:

- all staff (also Regional Board members, and anyone who accesses / uses data, in their work for the college)
- non-staff data subjects (current and former students; former staff, customers, and contractors).

2.3 This policy applies to all locations from which college data is accessed, including home use and overseas.

3.0 Objective

3.1 The college is committed to protecting the confidentiality, integrity and

availability of all information based on its intrinsic value and risk. UK GDPR stipulates the following approaches to ensure the security of personal data with an adequate level of protection:

Confidentiality	protecting information from unauthorised access and disclosure
Integrity	safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion
Availability	ensuring that information and associated services are available to authorised users whenever and wherever required
Resilience	the ability to restore the availability and access to information, processing systems and services in a timely manner in the event of a physical or technical incident

4.0 Responsibilities

4.1 The College is the Data Controller

4.2 **All users of college data are responsible for:**

- Following all college policies and procedures created by the College to ensure compliance with this policy.
- Completing mandatory and relevant Data Protection and Information Security training and awareness activities.
- Ensuring all data, and specifically personal and special category data, is processed securely
- Ensuring data is not disclosed to any unauthorised third party either accidentally or otherwise (including spoken disclosure)
- Reporting all suspected personal data breaches or incidents immediately to gdpr@borderscollege.ac.uk so appropriate action can be taken to minimise harm
- Leaving desks clear at the end of each working day, and paperwork locked away when not in use.
- Ensuring portable devices (laptops, memory sticks, and external hard drives) are not be left unattended. Memory sticks which hold personal data must be encrypted. These can be supplied by the helpdesk.
- Understanding and ensuring parents or guardians of students aged 13 and over only be given access to data relating to a student when the student has given permission for the release of information.
- Complying with the data protection principles set out in in section 5.

4.3 **The Vice Principal – Finance and Corporate Service**s is the executive lead.

4.4 **Strategic Leadership Team** are responsible for data handling within their teams in line with policy requirements.

4.5 The college has engaged a part-time Data Protection Officer (DPO) through HEFESTIS DPO Shared Services. The DPO is an advisor to the college and fulfils the statutory obligations of the role where empowered to do so. The DPO

can be contacted through the data protection mailbox: gdpr@borderscollege.ac.uk. Urgent queries can be directed to the HEFESTIS service by the Vice Principal.

4.6 **Staff members (in addition to 4.2)** are responsible for checking the information they provide to the college in connection with their employment is accurate and up to date and inform the college of changes.

4.7 **Students must:**

- Notify their tutor if they process personal data as part of their studies to ensure that they are processing in line with this policy.
- Ensure that all personal data provided to the college is accurate.
- Notifying the college of any changes to their address or personal details as provided at enrolment.

5.0 Legal Governance

5.1 Data Protection Principles

The college must process personal data according to the following six data protection principles:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject lawfulness, fairness and transparency.
2. Personal data shall be collected only for explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes purpose limitation.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed data minimisation.
4. Personal data shall be accurate and, where necessary, up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay accuracy.
5. Personal data shall be kept in a form which identifies data subjects for no longer than necessary for the purposes processed storage limitation.
6. Personal data shall be processed using appropriate technical or organisational measures that ensures appropriate data security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage integrity and confidentiality.

Details on how the College will meet these principles are in Annex B.

5.2 Accountability

5.2.1 Meeting the accountability requirements of data protection law allows the college to demonstrate compliance with the six principles above and provides assurance to individuals that their personal information is secure. The College

has the following accountability arrangements in place.

Data Protection Officer (DPO)	We have an appointed DPO who can be contacted via the data protection mailbox: gdpr@borderscollege.ac.uk
Policies and procedures	Policies and procedures to demonstrate appropriate technical and organisational security measures are in place.
Records of Processing Activities (Article 30 Register)	This covers the types of activities for each business area of the college where personal data is processed and the arrangements in place. This must be maintained and reviewed on a regular basis.
Data protection by design and default	When a policy, process or system involves personal data, the college builds in appropriate safeguards to protect the data from the start. This includes a Data Protection Impact Assessment process, to identify and mitigate privacy risks.
Agreement / Contract documentation	Ensuring appropriate contracts are in place with third-party organisations who process personal data on the college's behalf and where the college shares personal data with other organisations that this is properly documented in a data sharing agreement (DSA).
Training	All college staff and students must complete data protection and information security training.
Handling of data incidents / breaches	Robust detection, investigation and internal reporting procedures for data incident management and, where applicable, reporting to the Information Commissioner's Office (ICO) and data subjects affected within 72 hours of discovery. The DPO shall recommend, where necessary, actions to inform data subjects and reduce risks arising from the breach.

5.2.2 The accountability principle is an ongoing obligation; the college will regularly review and, where necessary, update documentation.

5.3 Rights of Data Subjects (Individuals)

5.3.1 Data subjects have a number of rights under data protection law:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

5.3.2 These rights are explained in further detail in **Annex C**. Some rights have conditions.

5.3.3 When an individual requests to exercise their rights, the request must be sent to the data protection mailbox gdpr@borderscollege.ac.uk and processed

within the legal timescale of one calendar month.

6.0 Compliance

6.1 Any deliberate breach of data protection policy may lead to disciplinary action, withdrawal of access to college facilities or even a criminal prosecution. Any questions about interpretation or operation of this policy should be raised with the Vice Principal or the DPO.

7.0 Related documents and further Reference

7.1 Engage Staff Induction and Compliance Training
7.2 Breach Notification Procedure
7.3 DPIA guidance
7.4 Privacy Notices
7.5 Information Security Policy
7.6 Electronic Systems Policy

The Data Protection Act 2018 is available here:
http://www.legislation.gov.uk/ukpga/2018/12/contents

The UK Information Commissioner's Office (ICO) website has a guide to GDPR https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ as well as guidance on information law.

This includes a guide to the Privacy and Electronic Communications Regulations (PECR) https://ico.org.uk/for-organisations/guide-to-pecr/

8.0 Review

8.1 This policy will be reviewed every 3 years or whenever legislation changes.

Appendix A

Definitions in Data Protection Law

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic data (fingerprint).

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data controller means the organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor means the organisation which processes personal data on behalf of the data controller. If an organisation is a data processor there are specific legal obligations; for example, you are required to maintain records of personal data and processing activities. You have legal liability if you are responsible for a breach.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample form the natural person in question.

Personal data means any information relating to an identifiable person (data subject); who can be directly or indirectly identified in particular by reference to an identifier. This definition is wide a means that a wide range of personal identifiers constitute personal data. This includes name, identification number (e.g. NI Number), location data, online identifier (IP address) which reflects the changes in technology and the way that organisations collect information about individuals. It also includes information relating to factors specific to the physical, physiological genetic, mental, economic, cultural or social identity of that individual.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing means any operation or set of operations which is performed on

personal data or on sets of personal data. Processing occurs whether it is electronic or physical records, it includes: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. So even if data is held in a server but not used this is still processing.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be identifiable without the use of additional information, provided. The additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data identifiable unless the additional information (e.g. use of a key code).

Recipient means a natural or legal person, public authority agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Special category data means personal data which identifies an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation. This data requires extra safeguards to protect it from unauthorised use, disclosure etc. as it is considered that this information can have a higher impact on the rights and freedoms of an individual. Criminal records and convictions information is not under this category of data but should also be handled with extra safeguards due to the sensitivity of the information. As required under data protection law, Annex D of this policy document relates to processing special category data.

Territorial Scope Data protection law applies to processing carried out by organisations operating within the UK. It also applies to organisations outside the UK that offer goods or services to individuals in the UK.

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Appendix B

How to apply the 6 Data Protection Principles:

Principle	This means that Borders College will
1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)	• Only collect and use personal data in accordance with the lawful conditions set down in data protection laws • Treat people fairly by using their personal data for specific purposes and in a way that they would reasonably expect. • Inform people how we use their personal data and what their rights are (known as a privacy notice). This includes being clear, open and honest about how the college uses their data to meet the requirements of the right to be informed. • Rely on an individual's consent, as the lawful basis for processing their personal data, only where: ✓ We've obtained the data subject's specific, informed and freely given consent. ✓ The individual has given consent, by a statement or a clear affirmative action (that we document). ✓ The individual has the right to withdraw their consent at any time without detriment to their interests. ✓ It is as easy to withdraw consent as it is to provide it.
2. Personal data shall be collected only for specified explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes (purpose limitation)	• Ensure that if we collect someone's personal data for one purpose (eg to provide advice on study skills), we will not reuse data for a different purpose that the individual did not agree to or expect (eg to promote goods and services for an external supplier) • Be clear as to the specific purposes of processing and ensure that the data subjects are fully informed • Ensure that if the data is to be used for another purpose it will be compatible with the original purpose.

Principle	This means that Borders College will
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)	• Only collect personal data that is sufficient for the stated purpose • Only collect the minimum data required, (i.e. we will not collect more personal data than is necessary for the purpose) • Reduce risks of disclosure by pseudonymising personal data where possible • Anonymise personal data wherever necessary and appropriate, (e.g. when using it for statistical purposes), so that individuals can no longer be identified • Review the data we hold and where appropriate delete what we do not need.
4. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy)	• Take all reasonable steps to ensure personal data is not incorrect and have a process in place to ensure that incorrect or misleading data is corrected or erased as soon as possible • Update personal data where appropriate, (eg when informed of a change of address, our records will be updated accordingly) • Ensure the accuracy of the personal data we create and record the source of that data (eg from data subject or from partner organisation) • Have processes in place to address an individual's right to rectification: how it is considered, actioned and recorded.
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)	• Only keep personal data for as long as necessary for the purpose required. • Apply the college's retention and disposal schedule in relation to all records and will regularly review the retention period for any records containing personal data • Have appropriate processes in place to comply with individuals' requests for erasure under the 'right to be forgotten'. • Destroy records securely in a manner appropriate to their format or anonymise the personal data when we no longer require it. • Identify personal data that needs to be kept for public interest archiving, scientific or historical research or statistical purposes.

Principle	This means that Borders College will
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (integrity and confidentiality)	• Have appropriate organisational security measures in place to protect personal data, including the Electronic Systems Policy and the Information Security Policy • Have appropriate technical security measures in place to protect personal data • Have appropriate physical and personnel security measures in place, (eg secure rooms where personal data is held) • Control access to personal data so that staff, contractors and others working in the college can only see the data that is necessary for them to fulfil their duties • Require all college staff, contractors, students and others who have access to personal data in the course of their work to complete data protection and information security training, supplemented by procedures and guidance relevant to their specific roles • Set and monitor compliance with security standards for the management of personal data as part of the college's framework of policies and procedures • Provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely when working away from the college • Where transferring personal data to another country outside the European Union (UK) put in place appropriate agreements and auditable security controls to maintain privacy rights • Make clear whether we use automated decision-making, including profiling, and if so the impact on them and their rights to object • Have robust detection, investigation and internal reporting procedures in place for data incident management • Where a data breach is likely to result in a high risk to the rights and freedoms of data subjects, the VP Finance and Corporate Services or the Data Protection Officer (DPO) shall liaise with the Information Commissioner's Office (ICO) and report the breach, in line with regulatory requirements, within 72 hours of discovery. The DPO shall also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

Appendix C

Data Subject Rights

Data Subject Right	This means that
Right to be informed	At the point that we collect individuals' personal data; we will explain to them in a clear, concise and accessible way the following: ✓Name and contact details of the college and the DPO ✓For what purposes we collect and use their personal data ✓What lawful conditions we rely on to process data and how this affects their rights ✓Our obligations to protect their personal data ✓What personal data we collect, including if special category data is collected ✓The sources from which we obtain data, if we have received the data from third parties ✓To whom we may disclose their data and why (eg with accrediting bodies like the SQA) ✓Which other countries we may send their data to, why we need to do this and what safeguards are in place ✓How long we retain data, and that it will be destroyed securely when no longer required ✓The rights in respect of the processing and how to exercise their rights including but not limited to: • The right to access • The right to object • The right to rectification • The right to withdraw consent (when consent has been used) • The right to lodge a complaint with the regulator – the UK ICO
	The college shall publish this information on its website and where appropriate in printed formats. The content of these Privacy Notices will be regularly reviewed and we will inform our data subjects of any significant changes that may affect them. Where we process personal data to keep people informed about college activities and events (ie marketing) we will provide in each communication a simple way for individuals to withdraw their consent for further marketing communications.

Data Subject Right	This means that
The right of access	Individuals have the right to request access to their personal data that the college holds. Any individual may make such a request and receive a copy of their information free of charge and within one month of their request.
Right to rectification	Individuals have the right to have inaccurate personal data rectified and incomplete personal data completed. We will provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them, such as home addresses.
The right to erasure	This is commonly known as the right to be forgotten. It means that individuals can have their personal data erased when it is no longer needed. This right only applies in certain circumstances and if there is an overriding legal obligation or public interest in continuing to process the data then the right cannot be met.
The right to restrict processing	Individuals may restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when the college no longer needs to keep personal data but the data subject needs the data for a legal claim.
The right to data portability	Where a data subject has provided personal data to the college by consent or contract for automated processing they have the right to request a machine-readable copy or have it sent to another data controller.
The right to object	All individuals have the right to object and prevent further processing of their data. This right is not absolute and requires certain conditions to be met. These conditions include: • if the college is processing personal data for direct marketing purposes an individual can object and the college must stop processing their data for marketing • if consent was given by or on behalf of a child for online services such as social media, they have the right to withdraw their consent and stop the college processing their data • where decisions have been taken solely by automated means then an individual can object, especially where such decisions could have a negative impact on them • the individual can object to processing which is carried out in the course of the college's legitimate interest or public interest, unless the college can demonstrate compelling lawful grounds for continuing to process the individual's data.

Data Subject Right	This means that
Rights in relation to automated decision making and profiling	A decision is made solely by automated means and without any human intervention. Profiling is automating processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process. This type of decision-making can only be carried out where the decision is necessary for the entry into or performance of a contract; authorised by law or based on the individual's explicit consent. When the college processes personal data which involves automated decision-making or profiling then it's important that the college: • provides the individual with information about the processing • provides a simple way for them to request human intervention or challenge a decision • carries out checks to ensure that the systems are working properly as intended.

Appendix D

Special Category and Criminal Offence data - Appropriate Policy Document

As part of Borders College data processing activities, we will process special category (Sensitive) and criminal offence data under the UK GDPR and the Data Protection Act 2018 (DPA 2018). The Act requires an Appropriate Policy Document (this Annex).

This Annex explains our processing and satisfies the requirements of the DPA 2018. It supplements the information already provided in this Data Protection Policy, the Record of Processing Activities (ROPA, Article 30 Register) and Privacy Notices.

1. Compliance with Principles

The College complies with the UK GDPR Principles, as outlined in this policy, at Section 5 and Annex B.

2. Processing activities and conditions

Conditions to process special categories of personal data:

2.1 Employment, social security and social protection purposes

- Health and Social care purposes - assessment of the working capacity of an employee
- Exercise of a function conferred by an enactment or rule of law
- Protecting the public against dishonesty, malpractice, or other seriously improper conduct.

Examples include, but are not limited to, staff sickness and absence management, disciplinary and grievance procedures, trade union membership.

2.2 Health or social care

- Health and Social Care purposes (a) occupational medicine and (b) assessment of working capacity of an employee

Examples include Occupational Health assessments and records.

2.3 Reasons of substantial public interest

- equality or opportunity of treatment
- exercise of a function conferred by an enactment or rule of law
- support for individuals with a particular disability or medical conditions
- safeguarding of children and of individuals at risk

Examples include equality monitoring and reporting, protected disclosures, development of personal learning support plans, personal emergency evacuation plans and safeguarding.

This also includes criminal offence data where the College has a statutory duty to protect children and vulnerable adults, as outlined in the Protection of Vulnerable Groups (Scotland) Act 2007 and the Disclosure (Scotland) Act 2020. The College will conduct criminal conviction checks to ensure that its staff or students undertaking regulated work do not pose a threat to the safety of children and vulnerable adults.

2.4 Other Special Category Processing

The College processes special category personal data in other instances where it is not a requirement under this policy. We provide clear and transparent information about why we process this data including our lawful basis in our privacy notices.

3. Retention and Destruction of Records

All special category and criminal offence data are retained in line with this Data Protection Policy and as detailed within the Record of Processing Activities (ROPA, Article 30 Register).

4. Policy Review

This document will be reviewed annually or updated as necessary where processing activities change

Status:	Approved
Policy Dated:	February 2025
Author:	Vice Principal – Finance & Corporate Services
Review Date:	January 2028
Equality Impact Assessed:	August 2021