Corporate Ref.	66
Level	Three
Senior Responsible Officer	Director of Communications, Policy & Research
Version	5
EIA	1 April 2018
Approved by	SMT
Approved date	10 November 2022
Superseded version	4
Review date	10 November 2025

Edinburgh College

Data Protection

Policy

Version Control

Version	Author	Date	Changes
5	Information Manager	04/10/2022	Revisions and reductions to 2018 policy (NB. should have been labelled version **4**); DPO reporting line amended to VP Corporate Development; moved to new template.

1. INTRODUCTION

This is the Edinburgh College Data Protection Policy. It sets out the legal framework and risks which govern our use of personal data; the College's commitment to protecting its personal data; and the obligations of users to protect personal data (with particular reference to special (previously called sensitive) categories of personal data). Definitions of personal data and special category data are provided in Appendix 1.

It applies to all managers, employees, contractors, and anyone else who can access or use data in their work for the College.

It should be read in conjunction with the policies listed in section 10.

Any concerns about the protection of data at Edinburgh College (or 'the College'), or non-compliance with this policy, must be reported to dataprotection@edinburghcollege.ac.uk immediately.

2. PURPOSE

In undertaking the business of Edinburgh College, we create, gather, store and process large amounts of information: this includes personal and special categories of personal data, which are subject to data protection laws.

The College is committed to protecting the confidentiality, integrity and availability of all information on the basis of its intrinsic value and risk, as set out in the College's Information Security Classification Policy.

In this policy the College confirms its commitment to protecting *personal data*, and to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

Protecting individuals' personal data, is consistent with college values ("trustworthy"). It is also consistent with the right to privacy expressed in both the European Convention on Human Rights (ECHR) (Article 8 provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions "in accordance with law" and "necessary in a democratic

society") and the UN Convention on the Rights of the Child (UNCRC) (Article 16: Every child has the right to privacy).

This policy, and associated policies and procedures, sets out data users' roles and obligations in protecting personal data, support the College's compliance with its obligations as a Data Controller (and where applicable, a Data Processor) under data protection legislation; and in managing risks to college personal data.

3. SCOPE

This policy applies to:

- All personal data created or received in the course of college business in all formats, of any age. "Personal Data" shall include personal and special category data.
- Personal data held or transmitted in physical (including paper) and electronic formats.
- Personal data transmitted in verbal format (e.g. in conversation, in a meeting, or over the telephone).

Who is affected by the policy:

- College staff (which includes contractors, temporary staff and anyone else who can access or use personal data, including special categories of data, in their work for the College).
- Non-staff data subjects (these include, but are not confined to: prospective applicants; applicants to programmes and posts; current and former students; alumni; former employees; family members where emergency or next of kin contacts are held, members of the Board of Management and Edinburgh College committees, volunteers, potential and actual donors, customers, people making requests for information or enquiries, complainants, professional contacts and representatives of funders, partners and contractors.

Where the policy applies:

- This policy applies to all locations from which college data are accessed, including home access and overseas.

4. OBJECTIVES

This policy sets out a framework of governance and accountability for data protection compliance across the College and the College's responsibilities for this under data protection legislation.

The Data Protection Policy forms part of the College's framework for Information Governance more broadly and should be read in conjunction with associated policies listed in section 10.

5. LEGAL GOVERANCE

The safe and secure management of personal data is integral to Edinburgh College's values and a key enabler of effective business practice.

However, beyond this, the College must comply with data protection legislation, including UK General Data Protection Regulation; UK Data Protection Act 2018 and Privacy and Electronic Communications Regulations (PECR). In addition, the College must comply with the European Union (EU) General Data Protection Regulation (GDPR) in relation to goods and services collected before 31 December 2020 and when offering goods and services to people in the EU or monitoring behaviour in the EU.

These data protection laws require the College to protect personal data and control how it is used in accordance with the legal rights of data subjects – the individuals whose personal and special category data is held.

5.1 Data Protection Principles

Under data protection law the College is responsible for, and must be able to demonstrate compliance with, the following data protection principles as set down in the UK General Data Protection

Regulation, and the Data Protection Act 2018. There are six Data Protection Principles.

5.1.1 Principle 1: Personal data shall be processed fairly, lawfully and transparently.

This means Edinburgh College will:

- Only collect and use personal data in accordance with the lawful conditions set down in data protection law and not breach other laws;
- Treat people fairly by using their personal data for specific purposes and in a way 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 transparency requirements of the right to be informed (for further detail please see section about individuals' rights);
- Rely on an individual's consent, as the legal basis for processing their personal data, only where:
    - We've obtained the data subject's specific, informed and freely-given consent; and
    - The individual has given consent, by a statement or a clear affirmative action (that we document); and
    - The individual has the right to withdraw their consent at any time without detriment to their interests; and it is as easy to withdraw consent as it is to provide it.

5.1.2 Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes ('purpose limitation').

This means Edinburgh College will:

- Ensure if we collect someone's personal data for one purpose (e.g. collecting a student's personal email address to correspond with them about an application for a programme of study), we will not reuse their data for a different purpose the individual did not agree to or expect (e.g. to promote goods and services for an external supplier);
- Be clear in the privacy notice as to the specific purposes of processing and ensure the data subjects are fully informed (for further information regarding right to be informed see section below on individuals' rights);
- Ensure, if the data is to be used for another purpose, it is compatible with the original purpose, or seek the individual's specific consent for the new purpose.

5.1.3 Principle 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').

This means Edinburgh College will:

- Only collect personal data sufficient and relevant for the stated purpose;
- Only collect the minimum data required, (i.e. we will not collect more personal data 'just in case');
- 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 individuals can no longer be identified;
- Review the data we hold and where appropriate delete what we do not need.

5.1.4 Principle 4: Personal data shall be accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

This means Edinburgh College will:

- Take all reasonable steps to ensure personal data is not incorrect and have processes in place to ensure incorrect or misleading data is corrected or erased as soon as possible;
- Update the personal data where appropriate, (e.g. 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 (e.g. 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.

5.1.5 Principle 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');

This means Edinburgh College will:

- Only keep personal data for as long as necessary for the purpose it was collected for;
- Apply the College's records management policy and 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 personal data 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.

5.1.6 Principle 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 organizational measures

Principle 6, known as the Security principle, relates to the 'CIA triad' - the confidentiality, integrity and availability of personal data and the systems which process personal data.

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

This means Edinburgh College will:

- Have appropriate *organisational* security measures in place to personal data (including policies, procedures and training);
- Have appropriate *technical* security measures in place to protect personal data;
- Have appropriate physical and personnel security measures in place, (e.g. secure rooms where personal data is held);
- Control access to personal data so staff, contractors and other people working in the College can only see the personal data 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 training, supplemented as

appropriate 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 information governance 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;
- Put in place appropriate agreements and auditable security controls where transferring personal data to another country outside the UK and European Union to maintain privacy rights;
- Have a robust security incident reporting procedure in place to manage, investigate and, where applicable, report to the Information Commissioner's Office and data subjects affected.
- Ensure the resilience of personal data processing systems and services, including the ability to continue to operate under adverse conditions (e.g. physical or technical incident); and ensure the College has the ability to restore these systems to an effective state.

In addition, the following apply at all times:

- All college users of data must ensure all personal and special category data they hold is kept securely;
- Users must ensure personal data is not disclosed to any unauthorised third party in any form either accidentally or otherwise (including verbal disclosure);
- Desks should be left clear at the end of each working day; paperwork will be locked away when not in use; portable devices (laptops, memory sticks, external hard drives) will not be left unattended.

5.1.7 Accountability

Edinburgh College must also meet an additional 'Accountability principle'; this principle compels the College to adopt policies and implement appropriate measures to ensure and demonstrate the processing of personal data complies with privacy law and the six principles above.

This includes the following:

- Records of Processing Activities. This will contain all the business functions of the College which collect personal data; the types of personal data collected; the source of the data; who (if any) it is shared with; the security measures in place to protect it; the retention and disposal of the data; the legal basis it is collected for and the conditions for processing. This must be maintained and reviewed on a regular basis;
- Adopting and implementing data protection policies and procedures that demonstrate appropriate technical and organisational security measures are in place;
- Appointing a Data Protection Officer (DPO); the College DPO can be contacted via the data protection mailbox dataprotection@edinburghcollege.ac.uk;
- Implementing a 'data protection by design and default' approach. This means whenever a policy, process or system involves personal data, the College considers and builds-in appropriate safeguards to protect the personal data from the start;
- Use proportionate privacy and information risk assessment, and where appropriate data protection impact assessment, to identify and mitigate privacy risks at each stage of every project or initiative involving processing personal data; and in managing upgrades or enhancements to systems and processes used to process personal data;
- Ensuring appropriate contracts are in place with any third-party organisations who process personal data on the College's behalf and where the College shares personal data

with other organisations this is properly documented in a data sharing agreement (DSA);
- Recording and where appropriate reporting personal data breaches to the regulator (UK Information Commissioner's Office (ICO)) and if necessary the affected data subjects;
- The College will adhere to relevant codes of conduct and where applicable sign up to certification schemes.

The accountability principle is an ongoing obligation, and the College shall regularly review (and where necessary update) documentation and risk assessments. Through meeting the accountability requirements, the College shall continue to meet its value of being trustworthy, with individuals being assured their personal information is secure.

5.2 Rights of Data Subjects (Individuals)

Individuals (data subjects) have rights under data protection law. These rights are explained in detail below and on the College's website.

The College has appropriate procedures in place to ensure these rights can be actioned if an individual makes a request.

It's important to note some rights have certain conditions that must be met for the rights to apply. All requests must be answered within one month (though this may be extended by a further two months in specific circumstances). Full guidance on how to respond to an individual making a request under data protection law (and when a request should be referred to the Information Management team) is available in the College's Data Protection Handbook on the College Staff Intranet (policies and procedures page).

5.2.1 Right to be informed

This means at the point we collect individuals' personal data, we will explain to them in a clear, concise and accessible way how we use their information. As a minimum, this will include who we are, why we use their information, who it is shared with, if it is sent outside of

the UK, how they can get in touch with us and how they can exercise their rights.

The College shall publish this information on its website and where appropriate in printed formats. We will review the content of these Privacy Notices regularly and 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 we will provide in each communication a simple way of withdrawing their consent to further marketing communications.

5.2.2 The right of access

This means individuals have the right to request access to their personal data held by the College and receive a copy of their information free of charge and within one month of their request (though the College may extend this by a further two months in specific circumstances).

5.2.3 Right to rectification

This means 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 we hold about them, such as home addresses.

5.2.4 The right to erasure

This is commonly known as the right to be forgotten. It means individuals can have their personal data erased when it is no longer needed, if the data has been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data.

5.2.5 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.

5.2.6 The right to data portability

This means 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.

5.2.7 The right to object

All individuals have the right to object and prevent further processing of their data in certain circumstances, including where the College is:

- Processing personal data for direct marketing;
- Processing data obtained for online services such as social media, where consent for the processing was previously given by or on behalf of a child, who withdraws their consent;
- Making a decision about them taken solely by automated means;
- Carrying out processing 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.

5.2.8 Rights in relation to automated decision-making and profiling

Automated individual decision-making means 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 the College shall:

- Provide the individual with information about the processing;
- Provide a simple way for them to request human intervention or challenge a decision;
- Carry out checks to ensure the systems are working as intended.

6. RISKS OF NON-COMPLIANCE

Misuse of personal data, through loss, disclosure or failure to comply with the data protection principles and the rights of data subjects, may result in significant legal, financial and reputational damage. It's important to note, in the event of personal or special category data breach individuals may claim compensation for damages caused by the breach.

Non-compliance with the data protection principles, or any concerns over data protection, must immediately be reported to dataprotection@edinburghcollege.ac.uk

7. AUTHORITY

This policy is issued under the authority of the Vice Principal, Corporate Development, who is also responsible for its interpretation and enforcement, and who may also delegate such authority to other people.

Users must comply with any reasonable written or verbal instruction issued by people with delegated authority in support of this policy. If users feel any such instructions are unreasonable or are not in support of these regulations, users may appeal to the Vice Principal,

Corporate Development within Edinburgh College or contact the College's independent Data Protection Officer.

8. LINES OF RESPONSIBILITY

8.1.1 All users of college information are responsible for:

- Following policies and procedures and completing relevant training and awareness activities provided by the college to support compliance with this policy;
- Taking all necessary steps to ensure no breaches of personal data result from their actions (taking into account personal data security principles in 5.1.6);
- Reporting all suspected personal data breaches or incidents immediately in line with the College's Information Security and Breach Policy;
- Taking all necessary steps to immediately limit and contain any damage to individuals which may, or has, resulted from a personal data breach;
- Complying with the data protection principles set out in in section 5;
- Informing the College of any changes to the information they have provided to the College in connection with their employment or studies, for instance, changes of address or bank account details.

8.1.2 Principal and Chief Executive

As the Chief Executive Officer of the College, the Principal has ultimate accountability for the College's compliance with data protection law.

8.1.3 Vice Principal, Corporate Development

The Vice Principal, Corporate Development has senior management accountability for data protection, reporting to the Principal and

Chief Executive and the Audit and Risk Assurance Committee on relevant risks and issues.

8.1.4 Information Management team

The Information Management team will support the College in its compliance with data protection law and the principles therein, through the provision of relevant advice, procedures, training, guidance and templates; and is responsible for ensuring procedures are in place for individuals to exercise any of their rights.

8.1.5 Data Protection Officer

The College has appointed an independent Data Protection Officer (DPO) in line with its duties, as a public authority, under data protection law.

In line with the duties set out under data protection law, the DPO will support the College in its compliance through the provision of independent advice and guidance; supporting the college to monitor internal compliance; providing advice regarding data protection impact assessments, and by acting as the first point of contact for data subjects and the Information Commissioner's Office (ICO).

In relation to personal data breaches and incidents, the College will consult with the DPO, who shall make recommendations to Edinburgh College with specific regard to a). whether to report a personal breach to the regulatory body (ICO); b). whether to report a personal data breach to the affected individual(s); and c). recommendations for further actions and preventative measures.

8.1.6 Senior Management team

Members of the Senior Management team are responsible for ensuring all staff manage their devolved responsibilities for compliance with this policy.

9. POLICY MONITORING AND EVALUATION

The Director of Communications, Policy and Research will report to the Vice Principal, Corporate Development; Information Governance Group, and Audit and Risk Assurance Committee any breaches of this policy which present data protection risks and issues and agree actions to address these.

The terms of this policy must be observed at all times. Any failure to comply with the terms of this policy may lead to disciplinary action being taken against the user in accordance with the College disciplinary policy and/or legal proceedings.

The type of disciplinary action taken will be dependent on the seriousness of the issue. Factors taken into account include:

- Breaches of confidentiality, security and the law;
- Damage to the college's reputation;
- Damage to data subjects' rights and/or freedoms;
- Creation of a hostile working environment.

The College reserves the right to:

- Pass information to the relevant statutory authorities;
- Withdraw a user's access to any IT system, including internet services.

The above list of sanctions is not exhaustive and may be altered or augmented by the College depending on the nature of the incident.

10. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

This policy should also be read in conjunction with the College's Disciplinary policies and procedures; the College Information Security and Breach Policy; Information Security Classification Policy; Data Protection Handbook; Special Category and Criminal

Convictions Personal Data Policy; the IT Facilities Acceptable Use Policy; and the Back-up and Archiving of Data Held on IT Systems Policy.

These policies and procedures are reviewed and updated as necessary to maintain an effective Information Governance Management System to meet the College's business needs and legal obligations.

Legal requirements and external standards

Data protection is subject to U.K. and European law and other relevant law in all jurisdictions in which the College operates.

All current UK Legislation is published at http://www.legislation.gov.uk/

The legislation listed below includes the key legislation on which this policy is based. It is important to note this is not an exhaustive list of legislation governing the college's wider operations.

UK Data Protection Act 2018	EU General Data Protection Regulation (EU GDPR)
UK General Data Protection Regulation (UK GDPR)	The Privacy and Electronic Communications Regulations (PECR) 2003
Freedom of Information (Scotland) Act 2002	Environmental Information (Scotland) Regulations 2004
The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019	

11. FURTHER HELP AND ADVICE

For further information and advice about this policy contact:

Email: dataprotection@edinburghcollege.ac.uk
Telephone: 0131 297 8663

APPENDIX 1 – DEFINITIONS IN DATA PROTECTION

The following provides a definition of the terminology used in this policy in relation to data protection law.

Availability means ensuring that personal data and associated services are available to authorised users whenever and wherever required.

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

Confidentiality means protecting personal data from unauthorised access and disclosure.

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 on you; for example, you are required to maintain records of personal data and processing activities. You will 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; (Art 4(6)).

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 (Art 4(13)).

Integrity means safeguarding the accuracy and completeness of personal data and preventing its unauthorised amendment or deletion.

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 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 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 (Art 4(12)).

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 the personal data can no longer be identifiable without the use of additional information, provided (e.g. use of a key code). The additional information is kept separately and is subject to technical and organisational measures.

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. (Art4(9)).

Resilience means the ability to restore the availability and access to personal data, processing systems and services in a timely manner in the event of a physical or technical incident.

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

Special category data (formerly known as sensitive personal 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 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.

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

Third party means a natural or legal person, public authority, or agency 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; (Art4(10)).

End of document