EDA COLLEGE

EDA College

EDUCATE | DEVELOP | ACHIEVE

DATA PROTECTION AND PRIVACY POLICY[1]

Version 1.0 | August 2025

Version Control/History

Policy Reference	EDA-POL-DPA-001
Version	1.0
Status	Approved
Approved by	Academic Board
Approval Date	August 2025
Effective Date	August 2025
Policy Owner	Principal
Data Protection Officer	Registrar
ICO Registration Number	ZB519374
Next Review Date	August 2026
Applies To	All staff, students, governors, contractors and volunteers

[1] *In accordance with UK GDPR, the Data Protection Act 2018 and ICO guidance*

Contents

1. Introduction and Purpose

EDA College ("the College") is committed to protecting the privacy and personal data of all individuals with whom it interacts, including students, staff, governors, applicants, alumni and external partners. We recognise that data protection is both a legal obligation and a matter of trust, and we are committed to handling personal data responsibly, transparently and securely.

This policy sets out how EDA College collects, uses, stores, shares and protects personal data in accordance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), and all other applicable data protection legislation. It applies to all personal data processed by the College, whether held electronically on paper or in any other format.

This policy applies to everyone who processes personal data on behalf of EDA College, including employees, governors, volunteers, students, contractors and agents. Compliance with this policy is mandatory. Breaches of this policy may result in disciplinary action and, where the breach involves a criminal offence under the DPA 2018, referral to the relevant authorities.

> "EDA College treats the protection of personal data as a core institutional responsibility. Every member of our community has a role to play in keeping data safe, and we are committed to continuous improvement in our data protection practices."

2. Legislative and Regulatory Framework

This policy has been prepared in accordance with:

Legislation / Regulation	Key Requirement
UK General Data Protection Regulation (UK GDPR)	The primary legislation governing the processing of personal data of individuals in the UK; sets out data protection principles, lawful bases for processing, and individual rights
Data Protection Act 2018 (DPA 2018)	Supplements and implements UK GDPR in domestic law; includes specific provisions for law enforcement, intelligence services and certain exemptions
Privacy and Electronic Communications Regulations 2003 (PECR)	Governs electronic marketing, cookies and confidentiality of electronic communications
Network and Information Systems Regulations 2018 (NIS Regulations)	Sets out cybersecurity requirements for certain organisations; relevant to the College's IT infrastructure obligations
Human Rights Act 1998 / ECHR Article 8	Protects the right to respect for private and family life; relevant to the proportionality of data processing activities
Freedom of Information Act 2000 (FOIA)	Gives individuals the right to request information held by public bodies; intersects with data protection where requests involve third-party personal data
ICO Guidance and Codes of Practice	Guidance issued by the Information Commissioner's Office, including codes on employment practices, CCTV, cookies, AI and special category data

3. Scope and Application

This policy applies to:

- All personal data processed by or on behalf of EDA College Ltd in any format (electronic, paper, audio, video or otherwise)
- All individuals who process personal data on behalf of EDA College, including: academic and professional services staff, governors and committee members, students (when processing personal data of third parties in the course of College activities), volunteers, contractors, agency workers and consultants
- All systems, devices and processes used to collect, store, use, share or delete personal data, whether managed by the College or by third-party processors on its behalf

This policy should be read alongside the College's specific Privacy Notices, which provide detailed information about how personal data is processed in particular contexts (e.g. student privacy notice, staff privacy notice, applicant privacy notice).

4. Definitions

The following definitions apply throughout this policy:

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual ('data subject'). This includes names, identification numbers, location data, online identifiers (e.g. IP addresses) and any factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data; biometric data (where used for identification); data concerning health; data concerning sex life or sexual orientation. This data requires additional safeguards.
Criminal offence data	Data relating to criminal convictions, offences or related security measures.
Data subject	The identified or identifiable living individual to whom personal data relates.
Data controller	An entity that determines the purposes and means of processing personal data. EDA College Ltd is a data controller in respect of personal data it processes.
Data processor	An entity that processes personal data on behalf of a data controller, under a written contract. Third-party providers such as the VLE provider or SMS provider may be data processors.
Processing	Any operation or set of operations performed on personal data, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, combination, restriction, erasure or destruction.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of their personal data. Consent must be as easy to withdraw as to give.
Legitimate interests	A lawful basis for processing where the College has a genuine and proportionate interest in processing the data, provided this is not overridden by the interests or rights of the data subject.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
ROPA	Records of Processing Activities: a document the College is required to maintain under UK GDPR Article 30, setting out all categories of processing activities carried out by the College.
DPIA	Data Protection Impact Assessment: a structured process for identifying and minimising data protection risks associated with a new or significantly changed processing activity.
ICO	Information Commissioner's Office: the UK's independent supervisory authority for data protection. EDA College is registered with the ICO as a data controller.
DPO	Data Protection Officer: the individual appointed by EDA College to advise on data protection compliance, monitor adherence to this policy, and act as a contact point for data subjects and the ICO.

5. Data Protection Principles

EDA College is committed to processing personal data in accordance with the seven data protection principles set out in Article 5 of UK GDPR. All personal data processed by the College must be:

Principle	What It Means	How EDA College Applies It
1. Lawfulness, fairness and transparency	Personal data must be processed lawfully, fairly and in a transparent manner	We publish Privacy Notices; we identify a lawful basis before processing; we do not use data in ways people would not reasonably expect

2. Purpose limitation	Personal data must be collected for specified, explicit and legitimate purposes and not processed in ways incompatible with those purposes	We document our processing purposes in our ROPA and Privacy Notices; we do not repurpose data without a fresh lawful basis
3. Data minimisation	Personal data must be adequate, relevant and limited to what is necessary	We only collect data we actually need; we regularly review data collections to remove unnecessary fields
4. Accuracy	Personal data must be accurate and, where necessary, kept up to date	We ask individuals to confirm and update their data; we have processes for correcting inaccurate data promptly
5. Storage limitation	Personal data must not be kept for longer than necessary	We maintain a Retention Schedule (Appendix A); we have processes for securely deleting data at the end of the retention period
6. Integrity and confidentiality	Personal data must be processed in a manner that ensures appropriate security	We implement technical and organisational security measures; we conduct regular security reviews; we train all staff
7. Accountability	The data controller must be able to demonstrate compliance with the principles	We maintain a ROPA, conduct DPIAs, appoint a DPO, deliver training, and review this policy annually

6. Lawful Basis for Processing

EDA College must identify a lawful basis before processing any personal data. The six lawful bases under UK GDPR Article 6 are set out below, together with the contexts in which EDA College relies on each:

Lawful Basis	When EDA College Relies on It	Examples
Contract	Processing is necessary for the performance of a contract with the data subject, or to take steps at the data subject's request before entering a contract	Processing student personal data to administer enrolment, assess fees, manage timetabling, record attendance and release results; processing employee data for payroll and HR administration
Legal obligation	Processing is necessary to comply with a legal obligation to which the College is subject	Reporting to the Student Loans Company; submitting statutory returns to HESA; complying with safeguarding duties; responding to court orders
Vital interests	Processing is necessary to protect the vital interests of the data subject or another person	Sharing health information in a medical emergency; informing next of kin in urgent welfare situations
Public task	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority	Certain elements of EDA College's academic and research activities
Legitimate interests	Processing is necessary for the College's legitimate interests (or those of a third party), provided these are not overridden by the data subject's interests or rights	Marketing communications to former students; fraud prevention; network and IT security monitoring; sharing data within the College for administrative purposes
Consent	The data subject has given clear, specific, freely given and unambiguous consent	Marketing to prospective students; optional student surveys; use of non-essential cookies; processing of special category data where another basis is not available

IMPORTANT: Where EDA College relies on consent as a lawful basis, individuals have the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing

carried out before the withdrawal. EDA College must make it as easy to withdraw consent as it is to give it.

7. Special Category Data

Special category data requires additional safeguards under UK GDPR Article 9 because of its sensitive nature. EDA College processes the following categories of special category data:

Category	Examples Processed by EDA College	Lawful Basis (Art. 6) and Condition (Art. 9)
Health data	Disability declarations, extenuating circumstances medical evidence, fitness to study information, occupational health referrals	Contract or Legal Obligation + Art. 9(2)(b) employment / Art. 9(2)(h) health or social care
Racial or ethnic origin	Equality monitoring data collected at enrolment and for OfS/HESA reporting	Consent (for monitoring) + Art. 9(2)(g) substantial public interest / Schedule 1 DPA 2018
Religious or philosophical beliefs	Equality monitoring; dietary requirements; religious observance requests	Consent + Art. 9(2)(g) substantial public interest
Sexual orientation	Equality monitoring data (optional disclosure)	Consent + Art. 9(2)(g) substantial public interest
Biometric data	Staff/student photo identification where used for verification purposes	Consent or substantial public interest
Criminal offence data	DBS check results for staff with student contact; disclosures required under safeguarding obligations	Legal Obligation + Art. 9(2)(g) / Schedule 1 DPA 2018

EDA College will only process special category data where a specific condition in UK GDPR Article 9(2) and the DPA 2018 Schedule 1 is met, and where appropriate safeguards are in place. Special category data will be accessible only to those with a genuine need and will be stored with enhanced security measures.

8. Personal Data We Collect and Process

EDA College collects and processes personal data about the following groups of individuals:

8.1 Students and Applicants

Category of Data	Examples	Source
Identity and contact	Full name, date of birth, address, email, phone, nationality	Provided by the individual on application or at enrolment
Academic records	Qualifications on entry, assessment grades, module results, transcripts, certificates	Generated during the course of study; provided by the individual
Attendance and engagement	Attendance records, VLE login activity, library usage	Generated automatically by College systems
Financial	Fee payment records, SLC reference numbers, bursary applications, bank details (self-funded)	Provided by the individual; SLC
Health and disability	Disability declarations, extenuating circumstances evidence, reasonable adjustment plans	Provided voluntarily by the individual
Equality monitoring	Ethnicity, religion, sexual orientation (all optional)	Provided voluntarily by the individual for monitoring purposes
Safeguarding	Welfare concerns, incident records, referrals	Generated in the course of pastoral support and safeguarding activity

Photographs and recordings	ID photographs, lecture recordings (where applicable)	Collected by the College with appropriate notice
IT usage	Login credentials, email communications, VLE activity, device usage on college networks	Generated automatically by college systems

8.2 Staff and Job Applicants

Category of Data	Examples	Source
Identity and contact	Full name, address, NI number, date of birth, emergency contacts	Provided by the individual during recruitment or on commencement
Employment records	Contract terms, pay, performance appraisals, leave records, absence, disciplinary records	Generated in the course of employment
Qualifications and references	Academic and professional qualifications, employment references	Provided by the individual and referees
Health	Occupational health records, sick leave records, reasonable adjustment plans	Provided by the individual and occupational health providers
DBS check results	Enhanced DBS certificate outcomes	Disclosure and Barring Service
Financial	Bank account details, payroll records, pension information, expenses	Provided by the individual; generated in the course of employment
IT usage	Email, VLE, system access logs	Generated automatically by College systems

8.3 Governors and Committee Members

EDA College processes identity, contact and governance-related data for governors, including declarations of interest, meeting attendance records and committee papers.

8.4 Alumni

EDA College retains limited contact and academic record data for alumni for the purposes of alumni engagement, graduate outcome tracking (as required by OfS), and testimonials (with consent).

8.5 Visitors, Contractors and External Partners

EDA College processes basic identity, contact and access-related data for visitors, contractors, suppliers and external partners to the extent necessary for the relevant relationship.

9. How We Use Personal Data

EDA College uses personal data for the following main purposes. The lawful basis for each use is indicated:

Purpose	Who It Applies To	Lawful Basis
Administering applications and enrolment	Students, applicants	Contract; Legal Obligation
Delivering teaching, learning and assessment	Students	Contract
Monitoring attendance and engagement	Students	Contract; Legal Obligation (SLC reporting)
Administering tuition fees and SLC funding	Students	Contract; Legal Obligation
Providing student support and pastoral care	Students	Contract; Vital Interests (in emergencies)

Managing extenuating circumstances and appeals	Students	Contract; Legal Obligation
Administering safeguarding and welfare concerns	Students, staff	Legal Obligation; Vital Interests
Employment administration (payroll, leave, appraisal)	Staff	Contract; Legal Obligation
Safer recruitment and DBS checking	Staff, applicants	Legal Obligation; Public Task
Equality monitoring and OfS/HESA reporting	Students, staff	Legal Obligation; Public Task; Consent (for sensitive categories)
Quality assurance and external examining	Students	Contract; Legitimate Interests
IT security and network monitoring	All users	Legitimate Interests
Marketing and outreach to prospective students	Prospective students	Consent; Legitimate Interests (where prior relationship exists)
Alumni engagement and graduate outcome tracking	Alumni	Legitimate Interests; Legal Obligation (OfS graduate outcomes)
Governance and Board administration	Governors	Contract; Legal Obligation
Fraud prevention and financial management	All	Legal Obligation; Legitimate Interests
Statutory reporting (OfS, SLC, HESA, DfE, ICO)	Students, staff	Legal Obligation

10. Data Sharing and Third-Party Processors

10.1 Sharing with Third Parties

EDA College shares personal data with third parties only where there is a lawful basis for doing so and only to the extent necessary. Third parties with whom we share data include:

Third Party	Data Shared	Basis for Sharing
Birmingham Newman University (Awarding Body)	Student identity, academic records, assessment data, attendance	Contract between EDA College and Newman University; contract between student and College
Student Loans Company (SLC) / Student Finance England	Student identity, enrolment status, attendance, fee information	Legal Obligation (SLC funding requirements)
Office for Students (OfS)	Student and staff data as required for regulatory returns	Legal Obligation
Higher Education Statistics Agency (HESA)	Student and staff data for statutory returns	Legal Obligation
Disclosure and Barring Service (DBS)	Staff identity for DBS checks	Legal Obligation; Safeguarding
HM Revenue & Customs (HMRC)	Staff payroll data, tax and NI information	Legal Obligation
Pension providers	Staff employment and payroll data	Contract; Legal Obligation
Ofsted / OfS inspectors	Documents and data required for inspection	Legal Obligation
External examiners	Anonymised or identified student assessment data	Contract; Legitimate Interests

IT service providers / cloud providers	Personal data stored or processed in College systems	Contract (as data processors)
Plagiarism detection services (e.g. Turnitin)	Student assessment submissions	Contract; Legitimate Interests
Health / wellbeing referral services	Limited health data with student consent	Consent; Vital Interests
Police / courts	Data required by law enforcement	Legal Obligation; Vital Interests

10.2 Data Processing Agreements

Where EDA College engages a third party to process personal data on its behalf (a 'data processor'), the College will ensure that a written Data Processing Agreement (DPA) is in place before any processing begins. The DPA will set out the subject matter, duration, nature and purpose of the processing, the type of personal data involved, and the obligations and rights of EDA College as controller.

EDA College will carry out due diligence on all new data processors, including reviewing their data protection practices and security measures, before appointing them.

10.3 What We Will NOT Do

- EDA College will not sell personal data to any third party
- EDA College will not share personal data with third parties for their own marketing purposes
- EDA College will not share personal data with third parties outside of those identified above without a lawful basis
- EDA College will not disclose personal data to family members, employers or other third parties without the data subject's consent, except where required by law

11. International Transfers of Personal Data

EDA College will not transfer personal data outside the United Kingdom (UK) unless:

- The country to which data is being transferred has been assessed by the UK Government as providing an adequate level of data protection (known as an 'adequacy decision')
- Appropriate safeguards are in place, such as International Data Transfer Agreements (IDTAs) or UK Addendum to the EU Standard Contractual Clauses
- The transfer falls within one of the limited derogations set out in UK GDPR Article 49 (e.g. explicit consent, contractual necessity)

Where EDA College uses cloud-based services (such as email platforms, VLEs or student management systems) that may store data outside the UK, the College will ensure that appropriate transfer mechanisms are in place and will record these in the ROPA.

> Staff and governors must not transfer personal data outside the UK (including by using personal cloud storage, overseas-based email services, or personal devices when travelling) without prior authorisation from the DPO.

12. Data Retention and Disposal

EDA College will not retain personal data for longer than is necessary for the purpose for which it was collected. The College's Retention Schedule (Appendix A) sets out the retention periods for each category of personal data held by the College.

12.1 Retention Principles

- Retention periods are determined by reference to: the purpose for which data was collected, any legal obligation to retain data for a specified period (e.g. HMRC requirements for payroll records, OfS requirements for student data), and the legitimate interests of the College in retaining data
- At the end of the retention period, personal data will be securely deleted or destroyed
- Paper records containing personal data will be disposed of using cross-cut shredding or confidential waste services
- Electronic data will be deleted in a manner that prevents recovery

- Third-party data processors will be required to confirm secure deletion of College data at the end of the processing relationship

12.2 Retention Schedule Summary

Data Category	Retention Period	Notes
Student academic records (transcripts, results)	6 years after programme completion, then archive permanently for degree-level awards	Degree certificates and transcripts are retained permanently
Student personal / contact data	6 years after leaving the College	Required for potential legal claims and SLC audit purposes
Student financial records	6 years after the end of the academic year	HMRC and SLC audit requirements
Student health / extenuating circumstances	Duration of studies + 3 years	Retained for appeals and regulatory purposes
Student safeguarding records	Until the student reaches age 25, or 7 years from creation (whichever is longer)	Minimum statutory requirements
Staff HR records (employment)	6 years after end of employment	Employment law limitation periods
Staff payroll and financial records	6 years after end of tax year	HMRC requirement
Staff DBS records	6 months after recruitment decision; outcome retained if required by law	ICO guidance on DBS records
Job applicant records (unsuccessful)	6 months after decision	Equality Act limitation period for claims
Governor records	6 years after end of term of office	Governance best practice
CCTV footage	15 days unless required for investigation	See Section 22
Website analytics data	13 months	ICO guidance on analytics cookies
Email communications	3 years (staff); duration of enrolment + 1 year (students)	Review annually; delete where no longer needed
Complaints and appeals records	6 years from final outcome	Limitation periods for legal claims

The full Retention Schedule is reviewed annually by the DPO and updated as required. Staff must not retain personal data beyond the periods set out in this schedule without authorisation from the DPO.

13. Data Security

EDA College is committed to implementing appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. The following security measures are in place:

13.1 Technical Security Measures

- Secure password policies and multi-factor authentication for all College systems
- Encrypted storage for sensitive personal data, including special category data
- Encrypted transmission of personal data over the internet (TLS/SSL)
- Regular software updates and patch management
- Antivirus and malware protection on all College devices
- Firewall and network security monitoring
- Role-based access controls, ensuring staff can only access data necessary for their role
- Regular automated data backups with tested recovery procedures

- Secure remote access provisions for staff working off-site
- Audit logging of access to sensitive systems and data

13.2 Organisational Security Measures

- Mandatory data protection training for all staff on joining and annually thereafter
- Clear desk and clear screen policies in all College offices
- Secure storage and restricted access for paper records containing personal data
- Confidential waste disposal using approved shredding services
- Secure visitor access procedures for College premises
- Contractual data protection obligations imposed on all data processors
- Annual review of IT security measures and data protection controls
- Incident response and data breach management procedures (see Section 19)

13.3 Personal Devices and Remote Working

Staff must not use personal devices to store or process College personal data unless the device is enrolled in the College's mobile device management system and approved by the IT Manager. Staff working remotely must access College data via approved secure channels only and must not store College personal data on personal cloud storage services.

> Any suspected data security incident — including loss of a device containing personal data, accidental disclosure, or suspected unauthorised access — must be reported to the DPO immediately, and no later than within one hour of discovery. See Section 19 and Appendix B for the full breach reporting procedure.

14. Your Rights as a Data Subject

UK GDPR gives individuals a number of rights in relation to their personal data. EDA College is committed to respecting and facilitating these rights. The rights available depend on the lawful basis for processing and the circumstances of the request.

Right	What It Means	How to Exercise It
Right to be informed	The right to receive clear and transparent information about how your personal data is used, provided through Privacy Notices	Privacy Notices are published on the College website and provided at enrolment / employment
Right of access (SAR)	The right to obtain a copy of your personal data held by the College, and information about how it is processed	Submit a Subject Access Request using the form at Appendix C or by emailing the DPO
Right to rectification	The right to have inaccurate personal data corrected or incomplete data completed	Contact the DPO or Academic Registrar; we will act within one month
Right to erasure ('right to be forgotten')	The right to have personal data deleted where it is no longer necessary, where consent is withdrawn, or in certain other circumstances. This right is not absolute.	Submit a request to the DPO; we will assess whether the right applies and respond within one month
Right to restrict processing	The right to request that the College stops using your data in certain circumstances (e.g. while accuracy is disputed)	Submit a request to the DPO; we will act within one month
Right to data portability	The right to receive your personal data in a structured, commonly used and machine-readable format, where processing is based on consent or contract and is carried out by automated means	Submit a request to the DPO; we will respond within one month
Right to object	The right to object to processing based on legitimate interests or for direct marketing purposes	Submit a request to the DPO; we will stop processing unless we have compelling legitimate grounds

Rights related to automated decision-making	The right not to be subject to solely automated decisions that have a significant effect, unless certain conditions apply	Contact the DPO; see Section 20 for EDA College's approach to automated decisions
Right to withdraw consent	Where processing is based on consent, the right to withdraw consent at any time without detriment	Contact the DPO or the relevant team; withdrawal will be actioned promptly

EDA College will respond to all data subject rights requests within one month of receipt. Where a request is complex or numerous, this period may be extended by up to two further months, with notice to the requester. Requests are free of charge unless manifestly unfounded or excessive.

> To exercise any of your data protection rights, please complete the Data Subject Rights Request Form (Appendix C) or contact the DPO using the details in Appendix D. You also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk if you believe your data protection rights have been breached.

15. The Data Protection Officer (DPO)

EDA College has appointed a Data Protection Officer (DPO) in accordance with UK GDPR Articles 37–39. The DPO is responsible for:

- Informing and advising EDA College and its staff about data protection obligations
- Monitoring compliance with UK GDPR, the DPA 2018 and this policy
- Advising on Data Protection Impact Assessments (DPIAs)
- Cooperating with the Information Commissioner's Office (ICO)
- Acting as the contact point for data subjects exercising their rights
- Acting as the contact point for the ICO on data protection matters
- Maintaining the Records of Processing Activities (ROPA)
- Delivering and overseeing staff data protection training
- Reviewing and updating this policy and associated procedures

The DPO operates independently and must not be instructed by EDA College on how to perform their DPO tasks. The DPO reports directly to the Board of Governors on data protection matters.

> The DPO's contact details are published on the College website and in Appendix D of this policy. All data protection queries, subject access requests and breach reports should be directed to the DPO in the first instance.

16. Privacy Notices

In accordance with the transparency principle (Section 5), EDA College provides Privacy Notices to all individuals whose personal data it processes. Privacy Notices set out in plain language: who is processing the data, what data is being processed, why it is being processed, the lawful basis, with whom data is shared, how long it will be kept, and what rights the individual has.

EDA College maintains and publishes the following Privacy Notices:

Privacy Notice	Audience	When Provided
Student Privacy Notice	All enrolled students and applicants	On application; at enrolment; when updated
Staff Privacy Notice	All employees, workers and contractors	On commencement of employment; when updated
Job Applicant Privacy Notice	All job applicants	At the point of application
Governor Privacy Notice	All governors and committee members	On appointment
Website Privacy Notice / Cookie Policy	All website visitors	On the College website; via cookie consent banner

CCTV Privacy Notice	All individuals on College premises	Via signage at camera locations
Alumni Privacy Notice	All alumni	On graduation; when the College makes contact
Visitor and Contractor Privacy Notice	Visitors, contractors and suppliers	On or before visiting College premises

All Privacy Notices are published on the College website and reviewed annually. Where a Privacy Notice is updated materially, affected individuals will be notified.

17. Records of Processing Activities (ROPA)

EDA College maintains a Record of Processing Activities (ROPA) in accordance with UK GDPR Article 30. The ROPA is a comprehensive internal document that records all personal data processing activities carried out by the College as a data controller.

The ROPA includes, for each processing activity:

- The name and contact details of the data controller and DPO
- The purposes of the processing
- A description of the categories of data subjects and personal data
- The categories of recipients to whom personal data has been or will be disclosed
- Details of any transfers to third countries
- The envisaged retention period
- A general description of technical and organisational security measures

The ROPA is maintained by the DPO, reviewed and updated at least annually, and made available to the ICO on request. Staff who introduce new processing activities or significantly change existing ones must notify the DPO to enable the ROPA to be updated.

18. Data Protection Impact Assessments (DPIA)

A Data Protection Impact Assessment (DPIA) is required before EDA College introduces any processing activity that is likely to result in a high risk to the rights and freedoms of individuals. A DPIA must be carried out for:

- New or significantly changed IT systems that process personal data
- Processing of special category data on a large scale
- Systematic monitoring of staff or student behaviour (e.g. enhanced attendance monitoring systems)
- The use of new technologies (including AI tools) that process personal data
- Processing that involves matching or combining datasets from different sources
- Processing of children's data
- Any other processing identified by the DPO as requiring a DPIA

The DPIA process involves: describing the processing, assessing necessity and proportionality, identifying and assessing risks, and identifying measures to mitigate those risks. The DPO must be consulted on all DPIAs. Where a DPIA identifies a high residual risk that cannot be mitigated, the ICO must be consulted before processing commences.

All staff proposing new processing activities or significant changes to existing activities must contact the DPO at the earliest opportunity to determine whether a DPIA is required.

19. Data Breach Management

A data breach is any security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Data breaches can result in significant harm to individuals and reputational and financial consequences for the College.

19.1 Types of Data Breach

- Confidentiality breach: unauthorised or accidental disclosure of personal data (e.g. sending an email to the wrong recipient; leaving a laptop on a train)

- Availability breach: accidental or unauthorised loss of access to personal data (e.g. a ransomware attack; accidental deletion of records)
- Integrity breach: unauthorised or accidental alteration of personal data

19.2 Reporting a Breach

ALL suspected or confirmed data breaches MUST be reported to the DPO immediately and no later than one hour after discovery. Do not attempt to investigate, conceal or resolve a breach without first reporting it to the DPO. See Appendix B for the full reporting procedure.

Step	Action	Timescale	Lead
1. Discover	Any person who discovers or suspects a data breach must report it to the DPO immediately	Immediately on discovery	All staff
2. Contain	DPO takes initial steps to contain the breach (e.g. change passwords, block access, retrieve documents)	Within 1 hour of discovery	DPO + IT Manager
3. Assess	DPO assesses the nature, scope and likely impact of the breach; determines whether ICO notification is required	Within 4 hours of discovery	DPO
4. Notify ICO	Where the breach is likely to result in a risk to individuals' rights and freedoms, notify the ICO within 72 hours of becoming aware	Within 72 hours of awareness	DPO + Principal
5. Notify individuals	Where the breach is likely to result in a HIGH risk to individuals, notify affected data subjects without undue delay	Without undue delay; after ICO notification if applicable	DPO + Principal
6. Document	Record the breach, its effects and the remedial action taken in the Breach Log, regardless of whether ICO notification is required	Within 72 hours	DPO
7. Review	Conduct post-incident review to identify root cause and prevent recurrence; report to Board of Governors	Within 30 days of breach resolution	DPO + Principal + Board

Not all breaches require notification to the ICO or affected individuals. The DPO will assess the risk level and determine the appropriate response. However, all breaches — however minor — must be reported internally to the DPO and recorded in the Breach Log.

20. Cookies and Website Data

EDA College's website uses cookies and similar tracking technologies. Our Cookie Policy, published on the College website, sets out:

- What cookies we use and why
- Which cookies are essential and which are optional
- How to manage your cookie preferences
- How long cookies are retained

In accordance with the Privacy and Electronic Communications Regulations 2003 (PECR) and ICO guidance, EDA College will:

- Request consent for non-essential cookies before placing them
- Make it as easy to refuse or withdraw consent as it is to give it
- Not set non-essential cookies until consent has been given
- Retain website analytics data for no longer than 13 months

21. CCTV and Surveillance

EDA College operates CCTV cameras on its premises for the purposes of crime prevention, security and the safety of staff, students and visitors. The College's CCTV system is operated in accordance with the ICO's CCTV Code of Practice and the following principles:

- CCTV cameras are positioned to capture only areas where monitoring is necessary and proportionate; cameras do not cover areas where individuals have a reasonable expectation of privacy (e.g. toilets, changing rooms)
- Clear signage is displayed at all CCTV camera locations, informing individuals that CCTV is in operation and providing the contact details of the DPO
- CCTV footage is retained for 15 days and then automatically overwritten, unless footage is required for an investigation, legal proceedings or a law enforcement request, in which case it will be retained for as long as necessary
- Access to CCTV footage is restricted to authorised personnel only; requests for access from police or other authorities will be dealt with by the DPO
- CCTV footage will not be shared with third parties without a lawful basis

Individuals have the right to request access to CCTV footage in which they appear. Such requests should be made to the DPO using the Subject Access Request form (Appendix C). Footage will be provided where it does not reveal personal data of other individuals, or will be appropriately redacted.

22. Staff Training and Accountability

EDA College recognises that data protection compliance depends on every member of staff understanding their obligations. The following training and accountability measures are in place:

Training / Activity	Audience	Frequency	Lead
Data protection induction module (mandatory)	All new staff before accessing personal data	On joining	DPO / HR
Annual data protection refresher training	All staff	Annually	DPO
Role-specific data protection training (e.g. HR, student records, IT)	Staff with heightened data access	On taking up the role; when significant changes occur	DPO
Data breach reporting training	All staff	At induction; refreshed annually	DPO / IT Manager
DPIA and records management training	Staff who introduce new processing activities	As required	DPO

Governor briefing on data protection obligations	All governors	On appointment; annually thereafter	DPO / Principal

Training completion is recorded and reported to the Academic Quality Committee and the Board of Governors annually. Failure to complete mandatory data protection training may result in restricted access to personal data systems until training is completed.

All staff are required to sign a Data Protection Acknowledgement confirming that they have read and understood this policy, as part of their induction process and annually thereafter.

23. Complaints and Enforcement

23.1 Internal Complaints

If you believe that EDA College has breached your data protection rights or this policy, you should raise your concern with the DPO in the first instance. The DPO will investigate and respond within one month. If you are not satisfied with the DPO's response, you may escalate to the Principal and ultimately to the Board of Governors.

23.2 ICO Complaints

You have the right to lodge a complaint with the Information Commissioner's Office (ICO) at any time if you believe that EDA College has failed to comply with UK GDPR or the DPA 2018. You do not need to exhaust the College's internal process first, though the ICO generally encourages individuals to raise concerns with the organisation first.

ICO Website	www.ico.org.uk
ICO Helpline	0303 123 1113
ICO Postal Address	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

23.3 Consequences of Breach

Breaches of this policy by EDA College staff may result in disciplinary action up to and including dismissal. Serious breaches may also result in:

- Criminal prosecution under the Data Protection Act 2018 (e.g. unlawful disclosure or obtaining of personal data)
- Civil claims by affected data subjects
- ICO enforcement action, including fines of up to £17.5 million or 4% of global annual turnover (whichever is higher) under UK GDPR
- Reputational damage to EDA College and loss of institutional trust

24. Monitoring, Review and Governance

This policy will be reviewed annually by the DPO and updated as necessary to reflect changes in legislation, ICO guidance or EDA College's processing activities. Material changes require approval by the Board of Governors.

Governance Activity	Lead	Frequency
Annual policy review and update	DPO	Annual (April each year)
Board approval of material policy changes	Board of Governors	As required
Annual data protection compliance report to Board	DPO	Annual
ROPA review and update	DPO	Annual; and when new processing begins
ICO registration review and renewal	DPO	Annual

Data processor due diligence reviews	DPO	Annual; and when new processors are engaged
Training completion reported to Academic Quality Committee	DPO / HR	Annual
Data breach log reviewed	DPO	Quarterly
CCTV system review	IT Manager / DPO	Annual
Cookie and Privacy Notice reviews	DPO	Annual; and when processing changes
Cyber security review	IT Manager	Annual

Appendix A: Data Retention Schedule

This schedule sets out the retention periods for each category of personal data held by EDA College. All periods run from the end of the relevant activity, relationship or event, unless otherwise stated.

Category	Retention Period	Legal Basis for Retention
Student academic records (degree transcripts, certificates)	Permanently (degree-level awards)	Public Interest; Awarding Body requirements
Student personal data (contact details, enrolment records)	6 years after leaving	Limitation Act 1980; SLC audit
Student assessment data (scripts, coursework)	1 year after results confirmed (then destroy)	Quality assurance purposes
Student financial records	6 years after end of academic year	HMRC; SLC audit requirements
Student extenuating circumstances / health records	Duration of studies + 3 years	Regulatory and appeals purposes
Student attendance and engagement records	Duration of studies + 3 years	SLC compliance; OfS reporting
Student safeguarding records	Until student reaches age 25 OR 7 years (whichever is longer)	Statutory safeguarding requirements
Student complaints and appeals records	6 years from final outcome	Limitation Act 1980
Student disciplinary records (minor)	Duration of studies + 1 year	Disciplinary purposes
Student disciplinary records (serious / expulsion)	6 years after leaving	Legal claims; regulatory purposes
Staff HR records (contract, appraisal, absence)	6 years after end of employment	Limitation Act 1980; Employment law
Staff payroll and pension records	6 years after end of tax year	HMRC requirements
Staff DBS certificate details	6 months after recruitment decision; outcome note if required by law	ICO DBS guidance
Unsuccessful job applicant records	6 months after decision	Equality Act 2010 limitation period
Governor records	6 years after end of term	Governance best practice
CCTV footage	15 days (unless retained for investigation)	ICO CCTV Code
Email communications (staff)	3 years (review and delete)	Legitimate interests; storage limitation
Website analytics	13 months	ICO analytics guidance
Contracts and legal documents	6 years after expiry	Limitation Act 1980
Financial records (general)	6 years after end of financial year	Companies Act; HMRC
Data breach records	5 years	ICO accountability requirement

Appendix B: Data Breach Reporting Procedure

This procedure must be followed by all EDA College staff when a data breach is discovered or suspected. Time is critical — please act immediately.

Step	Action Required	By When
STEP 1 REPORT	Contact the DPO immediately by phone or email. Do not attempt to investigate or resolve the breach yourself. Provide the following information: what happened, when you discovered it, what data may be affected, and how many people may be affected.	Immediately on discovery
STEP 2 CONTAIN	The DPO (with IT Manager if required) will take immediate steps to contain the breach: change passwords, revoke access, retrieve misdirected emails or documents, isolate affected systems.	Within 1 hour
STEP 3 ASSESS	The DPO will assess the breach: nature and scope, type of data involved, likely risk to individuals, whether the breach is notifiable to the ICO.	Within 4 hours
STEP 4 NOTIFY ICO	If the breach is likely to result in a risk to individuals' rights and freedoms, notify the ICO at ico.org.uk/report-a-breach within 72 hours of becoming aware. If 72 hours cannot be met, provide reasons for the delay. The DPO leads this notification with the Principal.	Within 72 hours of awareness
STEP 5 NOTIFY INDIVIDUALS	If the breach is likely to result in HIGH risk to individuals, notify affected data subjects without undue delay. The DPO will draft the notification with the Principal.	After ICO notification; without undue delay
STEP 6 DOCUMENT	Record the breach in the Data Breach Log regardless of whether ICO notification is required. Include: date, nature of breach, data involved, individuals affected, steps taken, outcome.	Within 72 hours of resolution
STEP 7 REVIEW	Conduct a post-incident review to identify root cause and prevent recurrence. Report findings to the Board of Governors at the next Board meeting.	Within 30 days

What counts as a reportable breach? Examples include: emailing personal data to the wrong recipient; losing a device (laptop, USB, phone) containing personal data; unauthorised access to student or staff records; a ransomware or phishing attack affecting personal data systems; sharing personal data with an unauthorised third party; leaving confidential documents in a public place.

> Not sure if it's a breach? Report it to the DPO anyway. It is always better to report and investigate than to fail to report a notifiable breach. Failure to report a breach internally can itself constitute a disciplinary matter.

Appendix C: Data Subject Rights Request Form

Use this form to exercise any of your data protection rights under UK GDPR. Submit to the DPO using the contact details in Appendix D. We will respond within one month of receipt.

YOUR DETAILS	
Full name	
Date of birth	
Email address	
Phone number	
Your relationship to EDA College (student / staff / alumni / other)	
TYPE OF REQUEST	
Please tick the right(s) you wish to exercise:	[ ] Subject Access Request — I want a copy of my personal data [ ] Rectification — I want inaccurate data corrected [ ] Erasure — I want my data deleted [ ] Restriction — I want processing of my data restricted [ ] Portability — I want my data in a portable format [ ] Objection — I want to object to processing of my data [ ] Withdraw Consent — I want to withdraw consent previously given [ ] Other — Please describe below
DETAILS OF YOUR REQUEST	
Please describe your request in as much detail as possible, including the specific data or processing activity you are asking about.	
Date range (if applicable)	From: To:
PROOF OF IDENTITY	
Please provide proof of your identity with this request.	Acceptable documents: copy of passport, driving licence, or other government-issued photo ID. We may also verify your identity by other means if the above is not available.
DECLARATION	
I confirm that the information provided in this form is accurate.	Signature / Name: Date:
FOR OFFICE USE ONLY	
Date received	
Identity verified	Yes / No
Date of response	
Outcome	
Handled by	

Appendix D: Key Contacts

Role	Contact Details	For Queries About
Data Protection Officer (DPO)	[Name to be confirmed] EDA College, Shirley, Birmingham Email: dpo@edacollege.ac.uk Phone: [To be confirmed]	All data protection queries; subject access requests; data breach reports; DPIAs; ROPA; policy questions
Academic Registrar	EDA College, Shirley, Birmingham Contact via College website	Student data queries; enrolment records; student rights requests relating to academic data
IT Manager	EDA College Ltd, Shirley, Birmingham Contact via College website	IT security incidents; CCTV; data system queries; remote access
Principal	EDA College Ltd, Shirley, Birmingham Contact via College website	Escalated data protection concerns; ICO notifications; Board reporting
Information Commissioner's Office (ICO)	www.ico.org.uk Helpline: 0303 123 1113 Wycliffe House, Water Lane, Wilmslow, SK9 5AF	ICO complaints; guidance on data protection rights; reporting breaches to the regulator

Approved by the Board of Governors of EDA College Ltd | August 2025

Educate. Develop. Achieve.