



2.0 Compliance

2.5 Data Protection and Retention Policy

Approved in Executive Office August 2022

Version Number 2

Reviewed by IT Manager August 2022



Version Control Statement

| Version | Date | Changes | Reason | Author | Next review |
|---------|----------|-------------------------------------|---------------|------------|-------------|
| 1 | Aug 2021 | New Policy | N/A | IT Manager | Aug 2022 |
| 2 | Aug 2022 | Grammar Check and minor adjustments | Annual Review | IT Manager | Aug 2023 |
| | | | | | |
| | | | | | |

External Reference Points

- General Data Protection Regulation (GDPR) as shown in Data Protection Act 2018
- Data Protection Act UK 2018
- Information Commissioner’s Office (UK) (ICO)

Related Policies and Documents

Affects all other policy documents. This document should however be read together with the following documents:

- Information Security Policy
- ICT Policy
- Information Advice and Guidance (IAG) Policy
- Incident Response Policy
- College Security Policy



Contents

| | |
|--|-----------|
| Data Protection Introduction | 4 |
| Scope | 4 |
| Personal data definitions | 4 |
| Data protection principles | 4 |
| Whose personal data does the College process? | 6 |
| Why does the College need to process personal data? | 6 |
| Uses of your Personal Information | 6 |
| Categories of Information held | 7 |
| <i>Special category (sensitive) personal data</i> | <i>7</i> |
| Sharing Personal Information | 7 |
| Accessing Your Personal Information | 8 |
| <i>Requests to delete personal data</i> | <i>8</i> |
| Complaints or Queries | 9 |
| Data Retention | 9 |
| <i>Data Retention Periods</i> | <i>9</i> |
| <i>Data Retention Periods – Guidelines for Staff</i> | <i>9</i> |
| Destruction and Disposal of Records and Data | 11 |
| <i>Paper Records</i> | <i>11</i> |
| <i>Electronic Records and Systems</i> | <i>11</i> |
| <i>Internal Correspondence</i> | <i>12</i> |
| Responsibilities | 12 |
| <i>Department Heads</i> | <i>12</i> |
| <i>Individual employees</i> | <i>12</i> |
| Compliance and Monitoring | 12 |
| External Reference Points | 13 |
| <i>Other Reference Points</i> | <i>13</i> |
| EDA College Subject Access Request Form | 14 |



Data Protection and Retention Policy

Data Protection Introduction

EDA College Limited (EDA) understands the importance of protecting personal information and is committed to fostering a culture of transparency and accountability by demonstrating compliance with the principles set out in the current legislation. This policy explains how the College uses personal data to remain compliant with the UK's Data Protection Act (2018) and the General Data Protection Regulation EU 2016/679 (GDPR).

EDA is the 'controller' of the personal data provided by staff, students and applicants, for the College to carry out its business effectively.

Scope

This policy applies to all personal data collected and processed by EDA in the conduct of its business.

Personal data definitions

Personal data is defined in the GDPR:

Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Special categories of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data protection principles

GDPR outlines six principles which underpin the handling of personal data. To ensure compliance with the Regulation, EDA must ensure that personal data is:

(1) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency).
In practice this means:



Having legitimate grounds for collecting and using personal data.

- Not using personal data in a way that would hurt the individual concerned.
- Being transparent about how the College intends to use personal data and provide privacy notices where appropriate.
- Handling personal data in a way that the individual would reasonably expect.
- Ensuring that the College does nothing unlawful with personal data.

(2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

In practice this means:

- Being clear about why the College is collecting personal data and what it intends to do with it.
- Providing privacy notices when collecting personal data.
- Ensuring that any additional processing of personal data is fair and only with explicit consent.

(3) Adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed (data minimisation).

In practice this means:

- Only processing the personal data that is necessary.

(4) Accurate and, where necessary, kept up to date (accurate).

In practice this means:

- Taking reasonable steps to ensure the accuracy of any personal data held.
- Ensuring that the source of the personal data is clear.
- Carefully consider any challenges to the accuracy of personal data.
- Considering whether it is necessary to update the information.

(5) Not kept for longer than is necessary for the purpose (storage limitation). (See appendix 2 for data retention periods)

In practice this means:

- Reviewing the length of time personal data is kept for.
- Considering the purpose, the College holds the personal data in deciding whether, and how long, it retains the information.
- Securely deleting information that is no longer needed.

(6) Processed in a manner that ensures the security of data using appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction (integrity and confidentiality).



In practice this means:

- Designing and organising security to fit the nature of the personal data held and the harm that may result from the breach.
- Ensuring that the right physical and security measures are in place, backed by robust policies and procedures and reliable, well-trained employees.
- Reporting security breaches promptly so that they can be reported to the Information Commissioner's Office within the required 72 hours timescale.

EDA, as the data controller, is responsible for and able to demonstrate compliance with these principles.

Whose personal data does the College process?

As a data controller, we process personal data about our learners, potential learners, tutors, all college staff, and any business contacts including other business partner contacts, consultants and legal advisors.

Why does the College need to process personal data?

- The College only processes personal data where this is necessary for fulfilling a service it has been contracted to provide
- Managing records
- Promoting services
- If required by law, including responding to law enforcement authorities and competent bodies to prevent or detect crime, fraud and money laundering

Uses of your Personal Information

EDA uses personal information to:

- to process applications, enrolments and workforce development programmes and contracts
- for the College's own internal records so that it can provide all concerned with a high-quality service
- to contact individuals in response to a specific enquiry
- to customise the College's services so they work better for individuals
- to contact individuals about services, products, offers and other things provided by the College that it thinks may be relevant
- To contact individuals via e-mail telephone or mail for research purposes.

At no time will the College assume permission to use information that is provided for anything other than the reasons stated here. The College may need to recommend internal transfers (signposting) to students (between the FE and HE provisions); and external transfers (to other colleges or organisations). In such instances, students will be requested to provide express permission for their information to be shared.



Categories of Information held

The categories of the information that the College collects, holds and shares include, but are not limited to:

- Personal information (such as name, student number, address, date of birth, national insurance number)
- Contact information (which may include a phone number, email and postal address)
- Educational Information (including qualifications, predicted grades, learning support needs, attendance information – number of absences and reasons and individual achievements)
- Characteristics (such as gender, age, ethnicity, nationality, and country of birth)
- Financial information (bank details)
- Information about personal preferences and interests
- Company information, (financial, staff, professional development records)
- Website usage data.

- Staff contract information (start dates, hours worked, post, roles and salary information, annual leave entitlement, employment history and professional development).

Special category (sensitive) personal data

EDA may collect and process special category data, only where necessary. The special category data we use is limited to:

- Evidence of physical or mental health or condition required to provide confirm eligibility for special learner adjustments. This may include evidence of any condition or needs such as a medical report, details of any needs relating to a disability, or learning difficulties. EDA will not process this information for any other purpose. Learners have a right to withdraw their consent for processing this special category information at any time except where the processing relates to an overriding legal or regulatory obligation placed upon EDA. Withdrawing consent for processing medical data may result in the withdrawal or refusal of learning support arrangements.
- EDA may collect and process information such as race, religion and ethnicity where we are legally required to report on statistics relating to equal opportunities, discrimination and diversity.

Sharing Personal Information

EDA does not sell, rent or lease its stakeholders' data to any third parties.

We may share data with trusted partners including:



- Awarding Bodies,
- Companies House,
- Department for Education,
- Office for Students (OFS),
- Education and Skills Funding Agency (ESFA),
- Quality Assurance Agency (QAA),
- Employers,
- HMRC,
- Higher Education Institutions,
- Local authorities,
- Ofsted,
- The Pension Service, Police, Social Care department, EDA Sub-contractors and Higher Education Statistics Agency (HESA).
- Police,
- Social Care department,
- EDA Sub-contractors and
- Higher Education Statistics Agency (HESA).

Accessing Your Personal Information

Individuals have the right to ask for a copy of any of their personal information held by EDA College Limited. They can make a 'subject access request' under the Data Protection Act 2018.

The easiest way to make a request is to complete the Subject Access Request Form, attached as Appendix 1 to our Data Protection and Retention Policy. A hard copy of this form is available upon request from the College. Alternatively, a request can be made directly to the college at dataprotection@edacollege.co.uk.

Requests to delete personal data

One of the key principles which underpin the GDPR is the right of an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This is also known as the right to be forgotten.

To make a request please contact the college on dataprotection@edacollege.co.uk

Any requests from individuals to:

- have inaccurate personal data rectified (right to rectification),
- restrict or suppress their personal data (right to restrict processing),
- obtain and reuse their data for their purposes across different services (right to data portability),
- object to how their data is used, should be made directly by e-mailing dataprotection@edacollege.co.uk



Complaints or Queries

If there are any questions about EDA’s collection and use of personal data, please contact us at dataprotection@EDA.ac.uk

If an individual has a concern about the way EDA has handled or is handling their personal information, or they wish to make a complaint because the College has not complied with its obligations, the individual can make a complaint internally through EDA’s Complaints procedure or externally to the Information Commissioners Office (ICO). Individuals should raise concerns within three months of their last meaningful contact with the College.

Details of how to do this are on the Information Commissioners Office website:

<https://ico.org.uk/concerns/handling>

By post: If the individual’s supporting evidence is in hard copy, they can print out the form and post it to the ICO (with supporting evidence) to:

Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF.

Data Retention

Data Retention forms an essential part of the personal data lifecycle. Data shall be maintained for as long as there is an operational need. The length of time it will be retained will be set out in the Data Retention Schedule

This document applies to the retention of personal data, which is processed and subsequently retained by EDA. It applies to all staff, contractors and temporary employees who hold or process any EDA records for any purpose. It applies equally to our servers, third-party servers, email accounts, and backup storage such as photographic, microform and electronic media that are used to store records as well as to more traditional paper or card records.

Data Retention Periods

Data Retention Periods – Guidelines for Staff

The College will not retain any personal information for longer than is required. In the table below, there are the guidelines for the staff in terms of the retention period and reasons for keeping that information along with the relevant legislation for their reference.

If a member of staff decides to keep personal information for longer than the periods indicated they must have a reason that is valid by reference to the Data Protection Principles and agree on this in writing with the Registrar.

| Type of Personal Information | Minimum Retention Period | Reasons |
|------------------------------|--------------------------|---------|
|------------------------------|--------------------------|---------|



| | | |
|--|---|---|
| Personnel files including training records. | 6 years from the end of employment. | References and potential litigation. |
| Staff application forms and interview notes for unsuccessful applicants. | 6 months from the date of the interview. | Sex Discrimination Act 1975, Race Relations Act 1976 and Disability Discrimination Act 1995. |
| Income Tax and NI returns, including correspondence with the tax office. | 6 years after the end of the financial year to which the records relate. | Income Tax (Employment) Regulations 1993. |
| Statutory Maternity Pay records and calculations. | 3 years after the end of the financial year to which the records relate. | Statutory Maternity Pay (General) Regulations 1986. |
| Statutory Sick Pay records and calculations. | Term of employment plus 40 years. | Social Security Contributions & Benefits Act 1952. |
| Wages and salary records. | Current year plus 6 years. | Taxes Management Act 1970, Limitation Act 1980, Equal Pay Act 1970, Minimum Wage Regulations 1998. |
| Accident books and records and reports of accidents. | Term of employment plus 40 years | Limitation Act 1980. |
| Health records. | During employment. | Management of Health and Safety at Work Regulations. |
| Health records where the reason for termination of employment is connected with health, including stress-related illness. | Term of employment plus 6 years. | Limitation Act 1980. |
| Medical records are kept because of the Control of Substances Hazardous to Health Regulations 1994. | Term of employment plus 40 years. | COSHH 1994, Control of Asbestos at Work Regulations 2002, Control of Lead at Work Regulations 2002, Control of Substances Hazardous to Health Regulations 2002. |
| Learner records, including academic achievements and conduct. All documentation relating to the delivery of ESF in the 2007-2013 period must be retained until 2022 at the earliest. | Registered student relationship with College plus 6 years | Limitation Act 1980. |
| CCTV Security Recordings | 07 days (unless investigation made and then as long as reasonably required for evidential purposes) | Potential investigation into incidents. |
| Contact details kept on personal files (e.g., card | Until it is apparent that the person is no longer | It is inaccurate processing if the information is held any |



| | | |
|--|---|---|
| index, Microsoft Outlook). | at the named location. | longer. |
| Personal information of any sort on a web page/site. | No longer than a period specifically agreed with the person. | The danger of inaccurate and irrelevant processing. |
| All supporting Documentation evidencing the delivery of the FE Provision | The Retention of Documents date is currently 31 December 2033 | |

Destruction and Disposal of Records and Data

All information of a confidential or sensitive nature on paper, card or electronic media must be securely destroyed when it is no longer required.

In compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, students and stakeholders; EDA’s policy and procedures aim to ensure the secure

and safe disposal of any confidential waste and information assets by our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

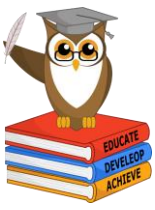
Paper Records

EDA in normal operational capacity retains paper-based personal information and as such, must ensure that it is disposed of in a secure, confidential and compliant manner. The College utilises an onsite-shredding device to dispose of all paper materials.

Electronic Records and Systems

EDA employs numerous systems, computers and technology equipment in the running of its programmes. From time to time, such assets must be disposed of and due to the information held on these whilst they are active; this disposal is handled ethically and securely. The deletion of electronic records must be organised in conjunction with the IT Manager who will ensure the removal of all data from the medium so that it cannot be reconstructed.

Only the IT Manager can authorise the disposal of any IT equipment. Where possible, information is wiped from the equipment through the use of software and formatting, however, this can still



leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

Internal Correspondence

Unless otherwise indicated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support (i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed). Where correspondence or memoranda that do not pertain to any documents have already been assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content cease or at a maximum, 2 years.

Examples of correspondence and routine memoranda include (but are not limited to):

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

When a data stick is found and handed to the IT manager for safekeeping it will remain there for 28 days. If after that period, the data stick is not claimed it will be disposed of.

Responsibilities

Department Heads

Heads of Departments have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (electronic or otherwise) and procedures they adopt, are managed in a way which meets the aims of this policy.

Individual employees

Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities and that they are maintained and disposed of by EDA College policy and procedure.

Compliance and Monitoring

EDA College is committed to ensuring continued compliance with this policy and any associated legislation and undertakes regular audits and monitoring of our records, their management, archiving and retention. Department Heads are tasked with ensuring the continued compliance and review of records and data within their remit.



External Reference Points

- General Data Protection Regulation (GDPR) as it applies in the UK
- Data Protection Act UK 2018
- Information Commissioner's Office (UK) (ICO)

Other Reference Points

- Sex Discrimination Act 1975,
- Race Relations Act 1976 and Disability Discrimination Act 1995.
- Income Tax (Employment) Regulations 1993.
- Statutory Maternity Pay (General) Regulations 1986.
- Social Security Contributions & Benefits Act 1952.
- Taxes Management Act 1970,
- Limitation Act 1980,
- Equal Pay Act 1970,
- Minimum Wage Regulations 1998.
- Limitation Act 1980.
- Management of Health and Safety at Work Regulations.
- COSHH 1994,
- Control of Asbestos at Work Regulations 2002,
- Control of Lead at Work Regulations 2002,
- Control of Substances Hazardous to Health Regulations 2002.



EDA College Subject Access Request Form

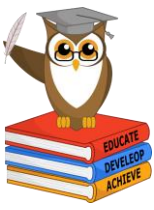
The following information is needed to help us give a quick and accurate response to your enquiry (within one calendar month). Please complete the information below and return it, to the Data Protection Team (contact details are provided below).

Part A. Please enter your details

| | |
|---|--|
| Title: | |
| Surname: | |
| Forename(s): | |
| Address: | |
| Telephone number: | |
| Email address: | |
| Another name by which you have been known, if applicable: | |
| Relationship to the College: | |

Part B. Declaration

Please describe your request and any further information which will enable us to locate your data (continue overleaf if necessary).



I am the Data Subject named in Part A of this document and hereby request, under the provisions of General Data Protection Regulation EU 2016/679 (GDPR), that EDA provide me with copies of my data as described in Part A.

Signed: _____ Date: _____

Part C. Proof of identity

The Data Protection Act requires the College to satisfy itself as to the identity of the person making the request. Please send a scanned copy of one form of identification containing a photograph (e.g. passport, photo card, driving licence) to EDA. If the supply of this documentation is problematic please contact us to consider alternative proof of identity arrangements. If the College is unable to satisfy itself as to your identity from the documentation you send us, we will contact you as soon as possible.

Return completed document by post to:
EDA Data Protection Officer
EDA College Limited
Balfour Business Centre 390-392 High Road ,
Ilford
IG1 1BF

Or by email to: dataprotection@edacollege.co.uk