Privacy and Data Governance Policy

Emil Dale ACADEMY

1. Aims

This policy aims to describe the principles and procedures that govern the management of data under all business streams of the Emil Dale Academy***, including the weekend school and all private sector hours of courses offered, and the arrangements for ensuring that data quality is maintained across the school.

****In this policy, the abbreviation of EDA will be used but covers all business streams of the Emil Dale Academy.*

2. Scope

Data protection is a legal compliance issue for EDA. EDA collect, store and process personal data about staff, pupils, students, parents, suppliers and third parties. It is recognised that the correct and lawful treatment of this data is integral in maintaining confidence in EDA, and relates directly to the successful running of the school.

The Data Governance Policy applies to data required for the management and administration of EDA and the conduct of its work, whether the data are captured and accessed from on or off-campus locations. It covers all staff working at EDA, whether paid or unpaid, regardless of their position, title, responsibilities, work experience, agency or peripatetic and volunteers. Specifically, the data covered by this policy relates to:

- Students and applicants (including those enrolled at the weekend school, free taster session and masterclasses);
- Staff;
- Governing Body;
- Curriculum Data;
- Research;
- Alumni and historical data;
- Finance;

Individual departments are responsible for the collection, management, maintenance and security of the data held at any given time, with careful consideration given to personal data and its identification in the inventory. It is good practice for an individual role holder to be identified within each department to act as the "data steward".

A Data Protection Officer oversees all procedures relating to good data management, including data security and protection. Any breaches of this policy may result in disciplinary action. Serious breaches of this policy may result in dismissal.

3. Terminology

- **Data Controller -** an organisation that determines the purpose of processing personal data. In this case, EDA is the controller of data relating to all students and staff. Responsibility then falls to EDA to safeguard all data.
- **Data Processor** - an organisation that processes data on behalf of a data controller.
- **Personal Data Breach** - a security breach that leads to accidental or unlawful destruction, loss, disclosure or access to personal data.
- **Personal Information (or Personal Data)** - any information relating to a person (including but not limited to their name, identification number, location or email) that can be used to identify them.
- **Processing** - any act relating to the personal data, including obtaining, collecting, organising, storing, internally sharing, altering and deleting.

- **Special Categories of Personal Data** - data relating to racial or ethnic origin, political opinions, religious beliefs, sexuality, health or medical conditions, genetic or biometric data used to identify an individual.

4. Principals

Data is used by EDA to benchmark and enhance all activities and services they offer. EDA may also be required to submit data to external bodies for statutory and/or regulatory purposes. To this end, the data collected by EDA must be of a high standard and quality, and must be regulated.

When devising this policy, references have been made to the principles of honesty, impartiality and rigour, as outlined by the HESA's data collection Codes of Practice, which applies equally to all data collections:

Principles of data preparation by higher education providers[1]
Honesty Data should genuinely reflect the characteristics, events, and objects being reported on, to the best of the HEP's ability. Processes and systems to collect, prepare, and submit data should be designed to enable this. Providers should be transparent in all discussions of the data, and not withhold information that bears on their accuracy or interpretation. The data collector should be informed promptly if errors are found after data has been submitted.
Impartiality Data should be collected, prepared, and submitted with impartiality and objectivity. This process should never be influenced by organisational, political, or personal interests. HE providers should implement controls to ensure that those dealing with data collections are protected from such interests.
Rigour Data should be collected, prepared, and submitted using repeatable and documented processes that can withstand scrutiny. When processes change, records should be kept of previous versions. Estimates and assumptions should be defensible, evidence-based, and documented, and the effect on the data tested. Assumptions and estimates should be reviewed regularly.

Close attention is also given to the six principles of GDPR relating to the processing of personal data which must be adhered to by data controllers and data processors alike. These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited to** what is necessary for the purpose it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of personal data.

5. Lawful Grounds for Data Processing

Under the GDPR, there are several recognised grounds for processing personal data, as seen above. Whilst consent is one, since regulations have been tightened, it is preferable to rely on another lawful ground where possible.

[1] Source https://www.hesa.ac.uk/innovation/data-landscape/Codes-of-practice/Supply-side

Legitimate interest is the most flexible basis for processing. This does require transparency, allowing data subjects to challenge the processing of their data. Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity
- a narrower set of ground for processing specific categories of personal data.

Legitimate interest must mean legitimate business interests in conducting and managing an effective working relationship. These relate to:

- personalising, enhancing, modifying or otherwise improving the services and/or communications that EDA can offer;
- promoting EDA services and studying how the website services are use, to develop them, grow the business and inform marketing strategies;
- safeguarding wellbeing and monitoring the progression of students, detecting and preventing fraud and operating a safe and lawful business;
- maintaining the School's reputation and standing as a Higher Education Provider;
- improving the security and optimisation of the network, site and services offered.

Where EDA processes information on the basis of legitimate interest, it is taken into account the impact it may have on the data subject. EDA's legitimate interest does not take precedent over the subject, and subjects can always exercise their rights should they believe the data processing is unlawful, unnecessary or invalid.

6. Ways EDA Collect Data

There are numerous ways that EDA may collect and process your personal data. Information may be collected about students/prospective students, staff/prospective staff and visitors when they:

- makes an enquiry is made, feedback is given or a complaint is made (this can be over the phone, by email or via the website;
- submit correspondence to EDA by post, email or via the website;
- apply for a course/register as a student
- attend a class, workshop, masterclass, audition, procution, event or other learning activity;
- attend an interview or audition as a prospective student for a full-time course;
- register and make a donation;
- update their personal information or account details;
- subscribe to the newsletter or mailing list;
- complete a form, conduct a search, post content to the website, respond to surveys, participate in promotions or use features of the website;
- provide or offer to provide EDA with goods or services;
- submit a CV or application for a job vacancy;
- attend an interview or assessment for a job vacancy;
- interact with social media accounts, including Facebook, Youtube, Twitter, Snapchat or Instagram.

7. What Information EDA May Collect

The data held by EDA about a person will vary depending on the interaction. EDA must ensure that all information collected is lawfully processed, as per the outlines above.

Information provided directly by applicants/students/staff
Information that EDA may collect includes, but is not limited to:

- identity and contact data: title, names, addresses, date of birth, email addresses and phone numbers;

- information on academic qualifications and statements concerning relevant experience, headshot photographs and other data items needed for monitoring purposes;
- student fees and funding: where a student or prospective student applies for a course, payment details may also be provided including billing address, credit/debit card details, bank account details and details of other financial information related to funding, such as eligibility for undergraduate grants, student loans, scholarships and bursaries;
- academic background data: for students/prospective students registering for a course or examinations, details of academic records, results and unique learner number may be stored;
- graduate records of auditions: successful applicants and offers from colleges may be used in promotional material;
- employment and background data: for job applicants, additional information may be provided relating to academic and work history, projects and research, previous income levels, references and other relevant details;
- survey data.

Information collected by EDA directly

Some information may be collected directly at the source by EDA. This may include, but is not limited to:

- information contained within correspondence: including contact over the phone, by email, or via the website;
- information transmitted on the website;
- information collected in person throughout the course of services;
- information collected during outreach workshops;
- transactional data: this includes the data, time, the amount charged and other related transaction details;
- website usage and technical data: EDA will record certain information about website use and the device used to access the site. This may include geographical location, device information (such as hardware model, mobile network information, unique device identifiers), the data transmitted by the browser (such as IP address, date and type of the request, content of the request regarding the specific site, time zone settings, access status/HTTP status code, volume of data transmitted, browser type and version, language settings, time zone settings referral source, length of visit to the website, date and time of the request, operating system and interface) number of page views, search queries and similar information. This information may be collected by a third party website analytics service provider on EDA's behalf and/or may be collected using cookies or similar technologies.
- imagery: EDA may film productions, spaces or capture imagery. Printed signage will be displayed whenever such filming or photography may occur;
- CCTV: information will be collected via CCTV footage which operates throughout the venue. Fixed signs at the entrances of EDA venues will inform visitors of the use of CCTV.

Special Categories

In some circumstances, EDA may need to collect special categories of personal data. Special categories of data include details on:

- race or ethnicity;
- religious or philosophical beliefs;
- gender;
- date of birth;
- income;
- sexual orientation or sex life;
- political opinion;
- trade union membership;
- health, genetic or biometric information;
- criminal convictions.

EDA must always provide further justification for collection, storing and using this type of personal information. Appropriate policy documents and safeguards that are required by law are also in place to ensure the safe handling of such information.

8. How EDA May Use Data Collected

EDA will use information for the purposes listed below either on the basis of:

- performance of a contract with EDA and the provision of their services to a subject;
- consent;
- to comply with legal or regulatory obligation;
- for legitimate interests.

The ways EDA may use data collected include, but are not limited to:

- monitoring attendance: for students attendance must be monitored through the data supplied by timetabling software and through the access card. This is to ensure attendance is in line with course requirements (to support EDA's legal obligation under UKBI's requirements for internal student visas, or on the basis of legitimate interests in safeguarding the wellbeing and monitoring the progression of students);
- processing and facilitating transactions: EDA will use information to process transactions and payments, to collect and recover money owed (on the basis of performing a contract and on the basis of legitimate interest to recover debts);
- tracking the effectiveness of outreach activity: information is collected from an attendant of a workshop, masterclass, event or audition (on the basis of EDA's legitimate interest to track the effectiveness of their activities);
- managing casting enquiries: records of past auditions are made to manage subsequent casting enquiries that EDA may receive we use records of your past auditions to manage subsequent casting enquiries we receive about you (on the basis of legitimate interest to track the casting of graduates and handle enquiries about graduates efficiently);
- managing relationships: this includes notifications on changes to terms of use, Privacy Notices, reviews, and surveys (on the basis of performing a contract and complying with legal obligations);
- supporting customers: to provide customer service and support (on the basis of a contract), deal with enquiries or complaints about the website and share information with our website developer, IT support provider, payment services provider as necessary to provide customer support (on the basis of our legitimate interest in providing the correct products and services to our customers and to comply with our legal obligations)
- fundraising: to identify individuals and organisations whose beliefs and values are aligned with the core work of our organisation for philanthropic support and for memberships (on the basis of legitimate interests as a registered charity to seek support and promote fundraising)
- facilitating prize draws, competitions and surveys: to enable students, staff, patrons and visitors to take part in prize draws, competitions and surveys (on the basis of performing a contract with legitimate interest in studying how the website and services are used, to develop them and grow the business)
- recruitment: to process any job applications submitted including sharing this with a third party recruitment agency (on the basis of legitimate interest to recruit new employees or contractors)
- marketing: to keep in contact with visitors about news, events, new website features products or services and fundraising opportunities that EDA believe may interest, provided that the requisite permission has been granted (either on the basis of consent where it has been requested, or legitimate interests to provide marketing communications it is lawful to do so). EDA will note marketing preferences so that only relevant or desired communication is received. These preferences can be updated at any time.
- advertising: to deliver relevant website content and advertisements and measure or understand the effectiveness of the advertising (on the basis of legitimate interests in studying how the website/services are used, to develop them, to grow the business and to inform EDA's marketing strategy)

- publicity: to promote the services on offer which may include photographs or films where you may appear. We may use such photographs or films in our printed and online publicity, social media and press releases (on the basis of our legitimate interests in promoting our services)
- analytics: to use data analytics to improve the website, products/services, marketing, customer relationships and experiences (on the basis of legitimate interests in defining types of customers for the website and services, to keep the website updated and relevant, to develop the business and inform EDA's marketing strategy)
- suggestions and recommendations: to share data collected with selected third parties such as suppliers and partners, to enable them to contact you with information about things that may interest you (where EDA have your consent to do so)
- research: to carry out aggregated and anonymised research about general engagement with the website (on the basis of legitimate interest in providing the right kinds of products and services to website users)
- compliance with policies, procedures and laws: to enable the compliance with policies and procedures outlined by the School, and to enforce EDA's legal rights, or to protect the rights, property or safety of employees and share personal details with our technical and legal advisors (on the basis of legitimate interest to operate a safe and lawful business or where there is a legal obligation to do so).

9. How Long Does EDA Keep Personal Information?

EDA will only hold personal information for as long as it is deemed necessary to fulfil legal duties, or business purposes. There may be a legal reason that personal information is held for a set period of time. Some data, eg the award of a degree to a named individual, will be kept in perpetuity.

10. Data Governance Standards

The collection, storage, processing and security of data at EDA must meet the required standards of data governance. In particular the data should be:

Defined consistently across all streams of EDA
Data collection processes must be clearly defined and stable to ensure consistency over time, so that data accurately and reliably reflects changes within EDA over time.

Collected for clearly defined and transparently communicated purposes
Data should only be collected when required for business or statutory purposes. Where applicable, these purposes should be communicated to data subjects via a privacy notice.

Stored in an official repository
Data must be held in a fit-for-purpose, rational, structured, backed-up format. Any duplication or internal sharing of data cannot take place without consent from the relevant Data Steward.

Readily available and easily accessible to all Data Users with a legitimate business need
Data access restrictions should be defined by staff role. Otherwise, data should be made accessible to staff under the principle of a time-based and demonstrable purpose relation directly to EDA.

Captured and entered only once, where possible
Data should be captured, or entered only once to avoid duplicate entries. A 'single source of truth' on all data subjects will help improve data accuracy.

Informed by thorough and effective updating processes

Data protection regulations require personal data to be accurate and up-to-date. Users with data editing access and responsibilities should receive the relevant training to ensure data quality and accuracy. Guidance for data subjects on how they can update their information should be provided at the point of capture.

Recorded in an auditable and traceable manner in accordance with any agreed change control processes
All changes to data should be logged and dated to ensure adherence to standards.

(In the case of personal data) Processed only where a legal basis for doing so has been identified and recorded
Data protection regulations - the GDPR - require organisations to enumerate clearly and accessibly the legal basis for processing any personal data. Data Stewards are responsible for the identification of personal data and the duration for which it is held. Privacy notices should also provide data subjects with information on the legal processing of their data.

(In the case of personal data) Only shared with external organisations where a data sharing agreement is in place
An indepth look on Data Sharing can be found below.

Stored securely
All data must be managed and stored efficiently. Access restrictions should be in place to govern the management of raw data sources and their back ups.

11. Data Sharing

EDA is committed to ensuring the security of its data assets, and the privacy of all those individuals - including, but not limited to, its students, staff, alumni, patrons and donors - whose personal data it collects and processes.

It is sometimes deemed necessary for EDA to share data with external organisations, for example, where there is a statutory requirement to do so, where such sharing is necessary for the administration of its programmes of study, or where there it is for the benefit or enhances the student experience.

Data sharing includes (but is not limited to):

- the sharing of data with a fellow Data Controller;
- the sharing of data with a Data Processor, who processes data on EDA's behalf;
- the one-off disclosure of data in an unexpected or emergency situation

When information is shared with an external organisation, the relevant Data Steward must determine if the organisation requesting the data is acting as a Data Processor (providing a service relation to personal data on behalf of the EDA), or a fellow Data Controller (receiving personal data to retain and manage). It is vital that EDA is able to disclose all recipients of personal data to data subjects if they submit a Subject Access Request.

Data Controllers

Where the sharing of personal data with another data controller is necessary, it is good practice to ensure that a data sharing agreement is in place with the third party. Data subjects should also be notified about the sharing of their personal information (for example, via a privacy notice). The notice should provide the details of when, and under what circumstances, EDA will share their data with third parties.

Data Processors

Data sharing with a third party data processor requires a written contract to be in place, which states the responsibility and liabilities of both parties. This contract should be authorised and signed by the relevant Data Manager. Contracts should outline the subject matter, duration of processing as well as the nature and purpose, the type of personal data and categories of data subject.

Contracts must also include as a minimum the following terms, requiring the process to:

- only act on the written instructions of the controller (in this case EDA);
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the proper consent of the controller, with a written contract;
- assist the controller in providing subjects access and allowing data subjects to exercise their rights under the General Data Protection Regulation (GDPR);
- assist the controller in meeting GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller when requested at the end of the contract;
- submit to audits and inspections, provide the controller with relevant information in a timely manner;
- to notify the controller of any infringement of GDPR or other data protection law

Ad-hoc Sharing

EDA acknowledges that situations can arise where it is necessary to share personal data, in an unexpected or emergency situation, for example, where the safety of a student or member of staff is at stake.

In circumstances such as these, it might not be possible to document the sharing. However, disclosures of personal data in situations like this are still subject to the relevant data protection legislation, and so it is good practice to make a record as soon as possible. The record should outline the circumstances, the date, what information was shared and the reason for disclosure.

Information Outside of the European Union

The majority of personal information is stored on systems in the UK or EU. However, there may be some occasions where personal information may leave the UK/EU, either to get to another organisation, or where it is stored in a system outside of the EU.

EDA will protect personal information in a range of secure ways, and will ensure that a robust contract is in place with the third party data processor.

12. Data Quality Standards

EDA must hold timely, accurate and reliable data, in order to manage and enhance the services offered, and to meet internal and external reporting requirements;

Specifically, EDA must ensure a high quality of data so that it can:

- provide effective and efficient services to students, staff and other stakeholders;
- inform student choice;
- produce comprehensive, purposeful and accurate management information on which decisions can be made to inform the future of the school;
- monitor and review its activities and operations;
- produce external returns to ensure accurate funding allocations, and demonstrate accountability to all stakeholders.

Key risks relation to data include:

- poor quality data giving a misleading impression to internal and external stakeholders of institutional performance in teaching and research;
- poor quality data resulting in inappropriate decision-making across the school;
- poor quality data resulting in reputational damage in areas such as student recruitment and access;
- inaccurate data leading to under/over-funding

All data held by EDA and any data collected to inform analysis and reporting must meet the required standards of data quality. In order to meet and maintain this standard, all staff members are encouraged to follow the principles of this policy when collecting and reporting any data.

Data Quality Principles

EDA outlines the following requirements for the collection of all data:

Accuracy

- ➔ Data should provide a clear representation of the activity/interaction

Completeness

- ➔ All data should be complete

Consistency

- ➔ Data collection processes must be clearly defined and stable to ensure consistency so that data accurately reflects any changes

Currency

- ➔ Data should remain available for the intended use within a reasonable or agreed time period

Precision

- ➔ Data should be sufficient in detail

Privacy

- ➔ Data must comply with the regulations on data protection and data security

Reasonableness

- ➔ Data should be relevant for the purposes for what it is used
- ➔ The amount of data collected should be proportionate to the value gained from it
- ➔ Data requirements should be specified and reviewed

Integrity

- ➔ Any redundant records should be disposed of

Timeliness

- ➔ Data should be collected and recorded as quickly as possible

Uniqueness

- ➔ Data should be captured only once

Validity

- ➔ Data should be recorded and used in accordance with the agreed requirements, rules and definitions to ensure integrity and consistency

Data Quality Objectives

The principles of data quality are supported by objectives set out below. EDA encourages all staff members to adhere to these objectives, across every stream of EDA.

1) **Appropriate Responsibility, Accountability and Awareness**
   - Every member of staff should recognise the need for good quality data and understand how they can

contribute to it;
- Every member of staff should be aware of their responsibilities with regard to data collection, storage, security, analysis and reporting;
- Every member of staff should be aware of the implications of poor data quality in the in their area, the implication and ramifications on their department and EDA as a whole;
- Every member of staff should report any systemic data quality issues immediately and ensure action is taken;
- Every member of staff should be aware of the policies related to security and data protection, and their impact on data quality.

2) **Appropriate Policies and Procedures**
- EDA must clearly define key data requirements and assurance arrangements;
- Local procedures must exist for all key activities such as major data collection exercises and statutory and external returns;
- All policies and procedures should be regularly reviewed to consider their impact on the quality of data, and changed where necessary;
- Departmental managers should ensure that all policies and procedures are adopted and embedded within the working processes and that compliance is achieved to the highest level, offering guidance when a member of staff is not meeting the required standard.

3) **Appropriate Systems and Processes**
- EDA must provide clear systems and business processes for data collection and reporting;
- Guidelines for all processes and supporting key documents should be readily available and adopted by all departments of EDA;
- Data collection systems should be validated internally to ensure accuracy;
- Where possible, systems should be electronic to reduce the risk of manual error, except where there is a need to collection, process and store original documents;
- EDA must provide clear strategies for data storage and archiving from systems.

4) **Appropriate Security**
- EDA must have in place appropriate security arrangements to ensure that data is protected from unauthorised access from outside the school.
- EDA must regulate access to data for all staff and students.

5) **Appropriate Staff Development**
- All staff members accessing, inputting and amending data for EDA should have the appropriate knowledge, competencies and capacity to carry out the activity and preserve data quality;
- All policies, procedures and guidelines should be communicated effectively to relevant staff, and this will include policies on security and data protection, as part of the wider consideration of data quality;
- Appropriate staff development and training will completed during staff induction but should also be made available to faculty members throughout the time of employment;
- Responsibility for data quality should be included in job descriptions with significant data handling or management responsibilities.

13. Individual’s Rights to their Personal Data

At any time, a subject access request can be made giving any person the right to obtain the information that EDA holds about them. When a subject access request is made, the Business & Strategy Manager must be informed.

EDA may be asked to:

- provide a person with a copy of all personal information held about them;
- correct personal information where it is inaccurate;
- delete personal information if a subject believes EDA should no longer be using it;
- transfer personal information to another provider;

- not use automated decision-making processes to make decisions about a subject.

There are very limited exceptions where a subject access request may be refused. Whilst it is not usual for an administrative fee to apply, EDA can ask for one if it is deemed the request is unfounded, repetitive or excessive. EDA will aim to respond to all legitimate requests within one month. Occasionally it may take longer than a month if the request is complex, or a number of requests have been made. EDA will notify the person on the status of their request, and regularly update them.

Requests must be made in writing to the below address:
Emil Dale Studios
60 Wilbury Way
Hitchin
SG4 0TA

14. Implementing the Policy

EDA aims to ensure that all staff are aware of their role and responsibility in relation to the creation, use, maintenance and disposal of data. In order to achieve this, the policy will be communicated to all faculty members whose role includes a data quality function. It is the responsibility of the line manager to ensure that all staff in their department handling data are aware of the policy and understand how it should inform their work.

Specialist training should be given to those with specific roles in relation to the collection, storage and use of personal data. Cross-institutional awareness is vital to ensure the regulations and legislation are adhered to.

Version Number	Date of Issue	Review Date	Author	Changes Made/ detail
01	22.01.2021	22.01.2022	Sarah Hooper	First draft