# The Edina Trust Data Protection Policy

## Introduction

The Edina Trust, which is a charity registered in Scotland (the charity), is committed to protecting the personal data of its employees, consultants, volunteers, trustees and grantees, and safely and securely processing their data in accordance with the General Data Protection Regulation (GDPR). This policy sets out how it does this and how it ensures that its employees, consultants, volunteers and trustees understand the rules governing their use of the personal data to which they have access in the course of their work. Under GDPR, the charity is the data controller as it does not use a third party to process its data and rarely shares its data with third parties. It follows the guidance from Information Commissioner’s Office (ICO), however, as a small charity, it is currently exempt from registration.

## Scope

This policy applies to all employees, consultants, volunteers and trustees who must be familiar with it, and comply with it fully at all times. You must notify the Data Protection Officer if you believe there has been a breach of this policy. GDPR compliance is very important, not least for the protection of personal data and an individual’s right to privacy, but because the consequences of non-compliance are serious. Failure to comply with any requirement within this policy may lead to disciplinary action under our procedures. This policy supplements our other policies relating to internet and email use. The charity will keep this policy under review and amend or change it as required.

## Who is responsible for this policy

The Trust’s Senior Administrator is the charity’s Data Protection Officer (DPO) and has overall responsibility for the day-to-day implementation of this policy. If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

## The Principles of Data Protection

The charity will comply with the principles of data protection contained within Article 5 of the EU General Data Protection Regulation. These state that all personal data processing shall be:

### 1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and organisations must be open and transparent as to how the data will be used.

### 2. Limited for its purpose

Data can only be collected for a specific, explicit and legitimate purpose. It cannot be re-used for any purpose that is incompatible with the original purpose for which it was collected.

### 3. Data minimisation

Any data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

### 4. Accurate

The data held must be accurate and kept up to date; inaccurate data must be erased or rectified without delay.

### 5. Retention

Data cannot be stored for longer than necessary for the purpose for which it is processed.

### 6. Integrity and confidentiality

The data held must be kept safe and secure, both physically and electronically.

# Ensuring Compliance with GDPR Principles

## **Principle 1:** **Data must be lawful, fair and transparent**

The charity has conducted an audit of the personal data that it holds on its subjects and is satisfied that any personal data held is lawful, fair and transparent. The charity will continue to conduct data audits from time to time, especially where new data processing activities arise, to ensure this remains the case.

### Privacy Notices and Statements

1. All of the charity’s consultants, volunteers, trustees and leavers are provided with Privacy Notices setting out the lawful bases on which their personal data is processed by the charity. Signed copies are retained to evidence compliance.

2. The charity’s grant application forms contain short Privacy Statement informing grantees of the lawful reason for processing their personal data and assurance that their personal data will not be shared with, or sold to, any outside organisation (unless otherwise stated). Personal data will be shared with the charity’s consultants located in the UK in line with the charity’s legitimate interests as a grant providing charity.

3. The charity’s Privacy Notice has been updated and is published on its website.

## **Principle 2: Data must be limited for its purpose**

Article 6 of the GDPR sets out the lawful bases on which personal information can be processed:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

The charity has examined all the personal data that it processes and has established the lawful basis on which each type of personal data is held. The matrix at Appendix 1 sets out the lawful bases for all the personal data held by the charity.

### Policy Statement Regarding Special Categories of Personal Data

This is more sensitive personal data that could create more significant risks to a person’s fundamental rights and freedoms e.g. put them at risk of discrimination. As such, this data requires more protection. The special categories include information about an individual’s:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Biometrics (where used for ID) | Ethnic origin | Politics | Health | Religion |
| Trade Union Membership | Genetics | Biometrics | Sexual orientation | Race |

The charity will only process special categories of personal data once it has established the additional lawful basis for doing so. The separate, additional lawful bases for the processing of special categories of personal data are set out in Article 9(2) of the GDPR and are listed at Appendix 2. If no Article 9 lawful basis applies, the charity will request the data subject's *explicit* consent to process the special personal data. Any such consent will clearly identify what the relevant special personal data is, why it is being processed and to whom it will be disclosed. An Article 30 Record of Special Categories of Data processed by the charity is included at Appendix 3.

This policy statement, along with Appendix 3, forms the charity’s Appropriate Policy Document for the processing of Special Category data.

## **Principle 3: Data must be minimised**

The charity only collects personal data which is relevant, adequate and limited in relation to what is necessary for the purpose for which it is processed. Appropriate information management systems are in place to avoid the duplication of personal data.

## **Principle 4: Data must be accurate**

The charity takes steps to ensure that any personal data it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. It will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Where inaccuracies are identified personal data will be rectified without delay.

### Subject Access Request

An individual can request to see what personal data is being held about them by the charity. Once the charity receives a Subject Access Request it will provide this information, free of charge, within a 28-day period. If complying with the request is complex, or requests are numerous, the deadline may be extended by two months, but the individual will be informed of this within the initial 28-day period. The charity can refuse to respond to certain requests, and in circumstances where the request is manifestly unfounded or excessive, can charge a fee.

### Right to Erasure

There are circumstances in which an individual can request the erasure of their personal data (see Appendix 4). Where one or more of these circumstances apply personal data will be erased without delay. If the personal data that needs to be erased has been passed onto other parties or recipients, the charity will contact them to inform them of their obligation to erase the personal data. If the individual asks, the charity must inform them of those recipients.

### Data portability requests

The charity will provide the personal data requested in a structured, commonly used and machine-readable format. The charity will provide this data either, to the individual who has requested it, or to the data controller they have requested it be sent to. This will be done free of charge, without delay and no later than one month after the request was submitted. This period can be extended to two months for complex or numerous requests, but the individual will be informed of the extension within one month.

## **Principle 5: Data Retention must be clearly justified**

The charity does not retain personal data for any longer than necessary for the purpose for which it is processed. Data subjects are informed of the retention periods via one of the charity’s Privacy Notices and statements listed on page 2. Retention periods are set out in the table below:

|  |  |
| --- | --- |
| **Category of data** | **Period Retained** |
| Job Applicants | If successful, duration of contract |
| If unsuccessful, 12 months |
| Leaver’s (ex-staff) records | Two years |
| Redacted leaver’s records | Four years |
| Disciplinary Records | Two years |
| Financial records | Six years |
| Trustee records | Six years |
| Health and Safety Records | Three years |
| Insurance policies | 40 years |
| Grant application forms | Grant scheme period plus 12 months |
| Photographs of pupils | Six years |

## **Principle 6: Integrity and confidentiality of data**

The charity has reviewed its IT systems and procedures to ensure that all reasonable measures are in place to ensure the personal data that it holds is kept safely and securely. The responsibilities of the charity’s IT Officer are set out below. There is a system of limited access to personal information held within HR files, both paper and electronic. All computers and laptops are password protected. There are appropriate back up and disaster recovery solutions in place. All staff and volunteers receive cybersecurity training, with refresher training provided, as deemed necessary by the IT Officer.

# Responsibilities under the Charity’s Data Protection Policy

## IT Officer Responsibilities in relation to Personal Data:

### **Ensure all systems, services, software and equipment meet acceptable security standards**

* Checking and scanning security hardware and software regularly to ensure it is functioning properly
* Researching third-party services, such as cloud services the company is considering using to store or process personal data

### **Storing personal data securely**

* The charity enforces a password policy which ensures users choose strong passwords. Passwords are changed annually, or whenever a password has/or may have been compromised.
* Personal data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
* The IT Officer and the DPO must approve any cloud service used to store personal data
* Servers containing personal data must be kept in a secure location, away from general office space
* Personal data should be regularly backed up in line with the company’s backup procedures
* As far as possible staff should avoid saving personal data directly to mobile devices such as laptops, tablets or smartphones
* All servers containing sensitive personal data must be approved and protected by security software
* All possible technical measures must be put in place to keep personal data secure

# Consultant, Volunteer and Trustee responsibilities in relation to Personal Data:

* Read, understand and sign the Staff Privacy notice
* Fully understand and comply with your data protection obligations under the charity Data Protection Policy
* Review the charity’s GDPR training materials; (if you require additional training on data protection matters please contact the DPO)
* Check that any personal data processing activities you are dealing with comply with our policy and are justified
* Do not use personal data in any unlawful way
* Do not store personal data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
* Comply with this policy at all times
* Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay
* In cases when personal data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
* Printed personal data should be shredded when it is no longer needed

# Data Protection Officer Responsibilities in relation to Personal Data:

* Keeping the Board of Trustees updated about data protection responsibilities, risks and issues
* Reviewing all data protection procedures and policies on a regular basis
* Arranging data protection training and advice for all staff members and others included in this policy
* Answering questions on data protection from staff, board members and other stakeholders
* Responding to individuals such as clients and employees who wish to know which personal data is being held on them by us
* Checking and approving, with third parties that handle the company’s personal data, any contracts or agreement regarding sensitive personal data processing

# Transfer of Personal Data Internationally

The charity’s work does not require the sharing of personal data of EU origin outside of the EU.

# Reporting Breaches

Any breach of this policy or of data protection laws must be reported to the DPO as soon as practically possible. The DPO will complete the Actual or Potential Data Protection Compliance Failure Report form (see Appendix 4). In line with the legal obligation, the charity will report any **serious[[1]](#footnote-1)** data breach to the ICO within 72 hours of discovery.

All consultants, volunteers and trustees have an obligation to report actual or potential data protection compliance failures. This allows us to:

* Investigate the failure and take remedial steps if necessary
* Maintain a Register of Compliance Failures (see Appendix 6)
* Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

# Appendix 1

**Lawful Bases for Processing Personal Data Matrix**



Lawful basis of processing consultant, volunteer, trustee, grantee and leaver data

Under Article 6 GDPR (personal data only)

|  |  |
| --- | --- |
| |  | | --- | |  | |
| **GPDR Ground for legal Processing (Article 6):** | **Likely information required/collected by the charity:** |
| Consent: the individual has given clear consent for you to process their personal data for a specific purpose. |  |
| For the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. | * Contact names, addresses, personal telephone numbers and personal email addresses for employee and emergency contacts * Any information or references obtained during recruitment * Details of the terms of employment and collective agreements * Payroll/tax and National Insurance information and bank details * Information about performance – current or prior * Pay rises or promotions * Details of job title and job duties, management, organisation of work * Health records * Absence records including holiday records, medical certificates, self-certification forms * Details of leave for family or personal reasons (e.g. maternity, paternity, shared parental or adoption leave); * Details of disciplinary investigations/proceedings * Details of grievance or complaints raised by employee, or by a third party about employee, whether or not any action was taken * Information on your membership of, or being a representative of, a trade union * Insurance details * Training records * Expense claims * Health and safety incidents * Access to employee/customer's property * Digital data on employee whereabouts including building access * Termination of employment details * Those with a high level of financial responsibility - “Independent background check” done every three years. * CVs, project reports, photos, |
| For compliance with a **legal obligation** to which the controller is subject. | * Contact names, addresses, personal telephone numbers and personal email addresses for employee and emergency contacts * Any information or references obtained during recruitment * Details of the terms of employment and collective agreements * Payroll/tax and National Insurance information. * Information about performance – current or prior * Details of job title and job duties, management, organisation of work * Health information * Details of disciplinary investigations/proceedings whether or not any disciplinary action was taken * Details of any grievances or complaints raised by employee, or by a third party about employee, whether or not any action was taken * Insurance details * Training records * Health and safety incidents * Access to employee/customer's property * Digital data on employee whereabouts including building access * Termination of employment details * Exit interview records * Timesheets |
| In order **to protect the vital interests of the data subject** or of another natural person. | * Contact names, addresses, personal telephone numbers and personal email addresses for employee and your of kin * Information or references obtained during recruitment which relate to the health/safety of the employee or risk to another person * Details of disciplinary investigations/proceedings if that discloses a risk to the vital interests of another person * Insurance details * Digital data on employee whereabouts including building access * Health and safety incidents * Health records * Travel insurance records * MOT certificate, registration number, business use insurance document, make & model of personal cars |
| For the **performance of a task** carried out in the public interest. | * Health and safety incidents * Monitoring on diversity |
| For the **purposes of the legitimate interests pursued by the controller** or by the third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.  **Edina Trust’s legitimate interest** is to enhance the teaching and learning of primary school science. | * Contact names, addresses, personal telephone numbers and personal email addresses for employee and your next of kin * Any information or references obtained during recruitment * Details of the terms of employment and collective agreements * Payroll/tax and National Insurance information and bank details * Information about performance – current or prior * Details of job title and job duties, management, organisation of work * information concerning your work contact details including telephone numbers, email addresses and professional social networking profiles * Health information * Access you may have to our property and how employee uses it * Details of disciplinary investigations/proceedings whether or not any disciplinary action was taken * Details of any grievances or complaints raised by employee, or by a third party about employee, whether or not any action was taken * Insurance details * Training records * Health and safety incidents * Monitoring on diversity * Digital data on your whereabouts including building access * Digital data on use of our telephone and IT systems including laptops, computers, tablets, smartphones, and other devices provided (in some circumstances this may include us monitoring) * Digital data on activity on business-related social networking sites * Digital data on access to our systems via your own personal devices where applicable (in some circumstances this may include us monitoring) * Communications with those responsible for managing you, others working with you and with Human Resources dept. E.g. if you make a flexible working request * Termination of employment details * Grantee’s contact names, email addresses (and telephone numbers if given) * Photographs of pupils using equipment supplied by ET * Using said photographs on Twitter and ET website to market grants to other schools (where explicit parental permission has been granted – confirmed by school) |

# 

# Appendix 2

# Lawful bases for Processing Special Categories of Personal Data

Special Categories of Personal data can be processed if:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f)  processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i)  processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j)  processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

# Appendix 3

Article 30 Record of Special Categories of Data Processed



Appendix 4

## Conditions which Permit an Individual to Request the Erasure of their Personal Data

1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
2. Where consent is withdrawn
3. Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
4. The personal data was unlawfully processed or otherwise breached data protection laws
5. To comply with a legal obligation
6. The processing relates to a child

## Dealing with the right to erasure

The charity can only refuse to comply with a right to erasure in the following circumstances:

* To exercise the right of freedom of expression and information
* To comply with a legal obligation for the performance of a public interest task or exercise of official authority
* For public health purposes in the public interest
* For archiving purposes in the public interest, scientific research, historical research or statistical purposes
* The exercise or defence of legal claims

Appendix 5

# Report form: Actual or Potential Data Protection Compliance Failure

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | **Date data breach identified** |  | | | **Person  reporting** |  |
| 2 | **Nature of personal data breach** | | | | | |
| **Actual or Potential data breach? NB Record which charity here** | | |  | | |
| **Details of breach** | | | | | |
| **Person who identified personal data breach?** | |  | | | |
| 3 | **Any remedial action taken to rectify actual or potential personal data breach?** | | | | | |
| 4 | **Any changes made to charity’s documents, policies and /or procedures in response to the personal data breach identified?** | | | | | |
| 5 | **Does the breach require to be reported to ICO?**  There is a legal requirement to report any compliance failures that are material in their own right or as part of a pattern of failures. | | | | | |
| 7 | **Does the personal data breach need to be reported to the Board of Trustees?**  Yes / No  **If yes, confirm when report given to the Trustees** | | | | | |
| 6 | **Confirmation of completed actions by Data Protection Officer**  I confirm that this breach has been reviewed and appropriate actions taken. I have added the breach to the relevant charity’s **Register of Compliance Failures**.  **Signed:** ------------------------------------------------------------- **Date:** --------------------------- | | | | | |

Version 01.05.2018

# Register of Compliance Failures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Brief summary of data breach** | **Cause of breach / how it occurred** | **Remedial Action taken** | **Date Trust Report form completed** | **ICO notified? Yes/No** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Appendix 6

1. Serious is considered to be a breach which is likely to result in a risk to the rights and freedoms of individuals and lead to discrimination, damage to reputation, financial loss, loss of confidentiality, or any other economic or social disadvantage. [↑](#footnote-ref-1)