



The de Ferrers Trust

DATA PROTECTION POLICY

| | |
|----------------------|---------------------|
| Author: | Director of Finance |
| Approval needed by: | Board of Directors |
| Adopted (date): | 15 May 2018 |
| Date of next review: | May 2019 |

Introduction

The de Ferrers Trust is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 2018. The Trust needs to process personal information about its staff, students, and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Any breach of the Data Protection Act 2018 or this Trust Data Protection Policy is considered to be an offence, and in that event relevant disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Trust, and who have access to personal information, will be expected to read and comply with this policy.

Background to the Data Protection Act 2018

The Data Protection Act 2018 brings into UK law the requirements of General Data Protection Regulations (“the GDPR”) which is a European Directive.

The GDPR (and hence the Data Protection Act 2018) exist to look after individual’s data and consist of a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The GDPR exists to protect individual rights in an increasingly digital world.

What is data?

Data is any information that relates to a living person which identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include personal opinions. The individual defined by the data is called the Data Subject.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

The Trust often collects sensitive data for the Department for Education and Local Authority requirements. Of course, student data may contain information about safeguarding, special education or health needs. Information about other family members may also be held.

Each Academy within the Trust has its own Privacy Notice for students which defines how personal information is processed, and which other organisations the personal

data will be shared with. These Privacy Notices are published on the relevant Academy's website, and are reviewed annually.

What are the key principles of the GDPR?

Lawfulness, transparency and fairness:

The Trust must have a legitimate reason to hold the data, this is explained in the Privacy Notices. Consent is often sought to use data about a student for a particular purpose. If an individual wishes to withdraw consent there is a form to complete to allow for the request to be processed. There are some circumstances when consent cannot be withdrawn.

Collect data for a specific purpose and use it for that purpose:

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection:

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. This ensures that, should there be a breach or a hack, only limited information can be lost.

Accuracy:

Data collected should be accurate, and steps should be taken to check and confirm accuracy. Data is collected when a student joins the Trust and the data is checked on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Data Controller or should not be held by the Data Controller in any event a dispute resolution process and complaint process can be accessed.

Retention:

The Trust has a retention policy that explains how long records are stored for.

Security:

Processes are in place to keep data safe. That might be paper files, electronic records or other information.

Data Subjects' rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected.

There are other rights that relate to automated decision making and data portability that are not directly relevant to Academies of Academy Trusts.

Data Subject's rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. The Trust also has legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

Individuals can ask for copies of information that is held about them or a student for whom they have parental responsibility by way of a Subject Access Request ("SAR").

Information requested must be provided within a month but this can be extended if, for example, the Academy was closed for holidays. The maximum extension permitted is two months.

When a request is received it may be necessary to ask the individual to be more specific about the information that they require in order to refine the information provided to ensure it is relevant to the actual query.

In some cases there will be contractual, legal or regulatory reasons which prevent all information held on file from being shared.

Information provided by a third party cannot be released without their consent.

Information will be supplied in an electronic form.

Who is a 'Data Controller'?

The Trust is the Data Controller (i.e. the Board of Directors). They have ultimate responsibility for how Trust manages data. They delegate this to Data Processors to act on their behalf.

Who is a 'Data Processor'?

A Data Processor is any person that uses, collects, accesses or amends the data that the Data Controller has collected or authorised to be collected. It can be a member of staff, a third-party company/service provider, a governor, a contractor or a temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Controllers must make sure that Data Processors are as careful with the data as the Data Controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

The Trust must have a reason to process the data about an individual. Privacy notices set out how we use data. The GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it must fall within one of those conditions.

If there is a data breach there is a protocol to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Data sharing

Data sharing is only carried out within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded on a case by case basis.

Breaches & non-compliance

Protecting data and maintaining data subjects' rights is the purpose of this policy and its associated procedures.

It is important that any potential or actual breach of any instance of non-compliance with this policy is brought to the attention of the Data Protection Officer to enable an action plan to be developed and implemented. This record will also serve as a useful mechanism to identify trends, risks and potential breach hazards.

By having an agreed timescale for review, identifying training needs that may be applicable to an individual or group of people will assist future compliance.

Consent

The Trust will seek consent from staff, volunteers, students, parents and carers to collect and process their data. The reasons for requesting the data (and how it will be used) will be made clear.

There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

Privacy Notices explain how data is collected and used.

Obtaining clear consent and ensuring that the consent remains in place is important for the Trust.

For Students and Parents/Carers

On joining an Academy within the Trust you will be asked to complete a form giving next of kin details, emergency contact and other essential information. You will also be asked to give consent for the use of that information for other in Trust purposes, as set out on the data collection/consent form.

The contact and consent form will be reviewed on an annual basis. It is important to inform the Academy/Trust if details or your decision about consent changes.

Pupil consent procedure

Where processing relates to a child under 16 years old, the Trust will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

CCTV policy

The Academies within the Trust may use CCTV and store images for a period of time in line with their local (Academy level) CCTV Policy.

CCTV may be used for:

- Detection and prevention of crime
- School staff disciplinary procedures
- Pupil behaviour and exclusion management processes
- To assist the school in complying with legal and regulatory obligations.

Data Protection Officer

We have a Data Protection Officer (“DPO”) whose role is to:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR

Our DPO is John Walker.

Physical security

In each Trust Academy, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied. Offices and cupboards that contain personal data should be secured if the Data Processor is not present.

The Premises Manager at each Academy is responsible for authorising access to secure areas along with Business/Office Manager (if different).

All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure GDPR and Data Protection Act 2018 compliance.

Complaints & the Information Commissioner Office (ICO)

The Trust has a Complaints Policy which deals with complaints about Data Protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

There is also a right to complain if you have requested that data is erased, rectified or not processed and that request has not been adequately dealt with.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk

Helpline: 0303 123 1113

web: www.ico.org.uk

Review

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every 12 months.