Forefield Junior School

MERSEY VIEW

Data Protection Policy

October 2024

Version Control

Version	Date	Status	Author	Comments
0.1	23.09.24	Draft	Trusts Choice	V1.1 standard policy
1.0	10.2024	Approved	Trust Board	Approved

Date of next review	

1. Related Policies

Mersey View Learning Trust (Trust) also adopts the following polices that relate to the Data Protection Policy:

- CCTV Policy
- Data Retention Schedule.

2. Introduction

The Trust is committed to being transparent about how it collects and uses the personal data of its staff, children, parents and carers and to meeting its data protection obligations.

This policy sets out the Trust's commitment to data protection, and individual rights and obligations in relation to personal data.

The Trust has appointed Schools Choice as its Data Protection Officer which role is to inform and advise the Trust on its data protection obligations. They can be contacted at data.protection@schoolschoice.org and questions about this policy, or requests for further information, may be directed to them.

Definitions

Personal data – any information that relates to an individual who can be identified from that information.
Processing – any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
Special categories of personal data – means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
Criminal records data – means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data Protection Principles

The Trust processes personal data in accordance with the following data protection principles:

- The Trust processes personal data lawfully, fairly and in a transparent manner.
- The Trust collects personal data only for specified, explicit and legitimate purposes.
- The Trust processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Trust keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Trust keeps personal data only for the period necessary for processing.
- The Trust adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Trust tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the Trust processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the UK General Data Protection Regulation (UK GDPR).

The Trust will update personal data promptly if an individual advises that their information has changed or is inaccurate and data gathered is held in:

- the individual's personnel file (in hard copy or electronic format, or both)
- on HR systems
- in child files.

The periods for which the Trust holds personal data are contained in its privacy notices/retention schedule and the Trust keeps a record of its processing activities in respect of personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

Privacy Notices

The Trust has a duty to check that staff, children, parents and carers information is accurate and up to date. It fulfils this by sending out a data collection form to parents/carers/staff on an annual basis.

This form will also include a privacy notice which outlines:

- who we are (including our contact details);
- the contact details of our Data Protection Officer;
- the purpose of the Trust processing data;
- the legal basis for processing data; and
- who this data will be shared with.

The current privacy notices for each relevant category of data subjects can be found on the Trust website.

4. Data Retention

The Trust maintains a retention schedule which can be found on the Trust's website.

This retention schedule is based on guidance from the Information and Records Management Society and it encompasses records managed by all types of Trust – some of the file descriptions listed may not be relevant to every Trust.

5. Individual Rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Trust will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located in territories outside of the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the Trust has failed to comply with their data protection rights; and
- whether or not the Trust carries out automated decision-making and the logic involved in any such decision-making (i.e. e-recruitment software).

The Trust will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should send the request to the Headteacher at the school [insert school head email address]. In some cases, the Trust may need to ask for proof of identification before the request can be processed. The Trust will inform the individual if it needs to verify their identity and the documents it requires.

The Trust will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Trust processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Trust will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the Trust is not obliged to comply with it. Alternatively, the Trust can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Trust has already responded. If an individual submits a request that is unfounded or excessive, the Trust will notify them that this is the case and whether or not it will respond to it.

Other Rights

Individuals have a number of other rights in relation to their personal data. They can require the Trust to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Trust's legitimate grounds for processing data (where the Trust relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Trust legitimate grounds for processing data.

To ask the Trust to take any of these steps, the individual should send the request to insert email address.

6. Disclosure of Personal Information

Information Sharing with Professionals Working with Children

Information sharing between professionals is vital to ensure the wellbeing of Children.

The Trust will follow the "7 golden rules of Information Sharing" described by the DfE:

1. Remember that the DPA/ UK GDPR is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf

7. Access to Pupils Records

Parents have two distinct rights to access information about their child held by a Trust.

These rights are:

1. The parent's right of access to their child's educational record under The Education (Pupil Information) Regulations 2005. A link to this document can be found here. http://www.legislation.gov.uk/uksi/2005/1437/contents/made
2. The pupil's right of subject access.

A child or young person will always be the owner of their personal information however if a young person is incapable of making their own decisions which is generally accepted as under the age of 12, the primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or young person.

The Trust will respond to a subject access request within 1 calendar month. If this request comes from someone other than the individual, the Trust will consider the capability of the individual and also must ensure the requester is acting the in the best interests of the individual.

Requests for information from pupils, or parents, for information that contains, wholly or partly, an educational record must receive a response within 15 working days.

Under the Regulations, requests from parents to view their child's educational record will be dealt with by the Board of Governors. All other requests for personal information from the pupil, or someone acting on their behalf, will be dealt with by the Head Teacher on behalf of the Trust.

8. International Data Transfers

The Trust will not transfer personal data to countries outside the UK.

9. Biometric Data

Biometric technologies are those which automatically measure people's physiological or behavioural characteristics. Examples include automatic fingerprint identification, iris and retina scanning, face recognition and hand geometry, and their use is becoming increasingly popular in educational settings.

Before the first processing of a child's biometric information, the Trust will notify each parent of the child:

- of its intention to process the child's biometric information
- that the parent may object at any time to the processing of the information.

10. Freedom of Information/Environmental Information Regulations

The Trust as a public authority is subject to The Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) and all requests for information that is not personal information must be treated as a FOI or EIR. These requests must be fully responded within 20 (school) working days by law. The information will be provided unless the Trust can provide an exemption or exception under the FOI act or EIR respectively.

In line with FOI regulations the Trust is required to have a publication scheme showing what information is held and how you can access this. The Trust's publication scheme can be found on the Trust website.

11. Data Security

The Trust takes the security of personal data seriously. The Trust has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Trust engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

An Information Risk Register will be created and maintained by each school which summarises each information asset schools maintain. Appropriate measures will be taken to mitigate the risk of disclosure of each information asset based on the impact level assigned.

12. Privacy Impact Assessments

Some of the processing that the Trust carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Trust will carry out a data privacy impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

13. Data Breaches

If the Trust discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery.

The Trust will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

14. Individual Responsibilities

Individuals are responsible for helping the Trust keep their personal data up to date. Individuals should let the Trust know if data provided to the Trust changes, for example if an individual moves house.

Individuals may have access to the personal data of other individuals in the course of their employment. Where this is the case, the Trust relies on individuals to help meet its data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Trust) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Trust's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Trust's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

15. Training

The Trust will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

16. Roles and Responsibilities

The senior information risk owner (SIRO) for the Trust is the Chief Executive Officer.

They are responsible for:

- Owning and updating this policy
- Owning the risk register
- Advocating information risk management and raising awareness of information security issues.

All staff are responsible for ensuring that information is managed according to this policy.