Godmanchester Community Education Trust

Data Protection Policy

April 2018

1. Introduction

Godmanchester Community Education Trust ("the Trust") is committed to a policy of protecting the rights and privacy of individuals, including pupils and others, in accordance with prevailing data protection legislation.

This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data. This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the General Data Protection Regulation ("GDPR") and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

This policy complies with our funding agreement and articles of association.

3. Relationship with existing policies

This policy has been drawn up within the context of:

- the Freedom of Information Scheme
- the Data Retention Policy
- and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the Trust and its schools.

4. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Special categories of personal data	Data such as: • contact details • racial or ethnic origin • political opinions • religious beliefs, or beliefs of a similar nature • whether a person is a member of a trade union • physical and mental health • sex life or sexual orientation • genetic or biometric data

Criminal records data	Data such as: • whether a person has committed, or is alleged to have committed, an offence • criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person or entity, other than an employee of the data controller, who processes the data on behalf of the data controller
Data protection officer	A person, other than an employee of the data controller, who oversees the implementation of data protection requirements at the Trust

5. The Data Controller

The Trust processes personal information relating to pupils, staff and visitors and is therefore a data controller. The Trust delegates the day to day responsibility for adhering to this policy to key personnel within the Trust. The Trust has also appointed a Data Protection Officer who is external to the Trust to oversee the implementation of this policy.

The Trust and its schools are registered as a data controller with the Information Commissioner's Office and renew these registrations annually.

6. Data Protection Principles

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

- Processing personal data lawfully, fairly and in a transparent manner.
- Collecting personal data only for specified, explicit and legitimate purposes.
- Processing personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeping accurate personal data and taking all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Keeping personal data only for the period necessary for processing.
- Adopting 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.

The Trust keeps a record of its processing activities in respect of personal data in accordance with the requirements of the GDPR.

7. Roles and responsibilities

The Board of Directors has overall responsibility for ensuring that the Trust complies with its obligations data protection legislation. The Executive Headteacher is responsible to the Board of Directors for ensuring, as far as is reasonably practicable, that the Trust and its schools comply with the GDPR. In order to discharge this responsibility the Executive Headteacher delegates duties and authority on a day-to-day basis to the Heads of School.

The Executive Headteacher and Heads of School will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

The Data Protection Officer will ensure the Trust has the correct and current regulations, audit the Trust and its schools annually for compliance with the latest regulations and advice.

The Administration Manager for the Trust checks that each school complies with this policy by, among other things, reviewing school records termly. Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy.

8. Privacy Notices

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how each school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as local authorities and the Department for Education, so that they are able to meet their statutory obligations.

More information can be found within the **GCET Privacy Notice - Pupils**.

9. Subject access requests

Under data protection legislation, pupils have a right to request access to information the Trust and its schools hold about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter or email. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The Trust will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupil's educational record will be normally provided within 15 school days (see (10) below).

If a subject access request does not relate to the educational record, we will respond within one month.

10. Parental requests to see the educational record

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at schools within the Trust may be granted without the express permission of the pupil.

Parents of pupils at schools within the Trust do not have an automatic right to access their child's educational record. The Trust will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office. Considerations will be made according to the ICO guidance of the following, among other things:

- where possible, the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;

- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

11. Storage of records

Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.

Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access, unless there is a clear medical reason and that there is explicit written consent i.e. allergy advice in school kitchens.

Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office.

Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.

Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

Staff, pupils, directors, members or governors who store personal information on their personal devices are expected to follow the same security procedures required for school-owned equipment.

12. Disposal of records

Personal information is kept for the term specified in the Data Retention policy. Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred (using a cross-shredder) or incinerate paper-based records and override electronic files. We may also use an outside company to safely dispose of electronic records.

13. Training

Our staff, directors, members and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation or the Trust or school's processes make it necessary.

14. Monitoring arrangements

The Executive Headteacher is responsible for monitoring and reviewing this policy. This document will be reviewed every two years or when there are changes to legal requirements or best practice in relation to data protection.

Signed: Phil Mackay Chair of Board of Directors On behalf of the GCET Board of Directors

Signed: Rod Warsap Executive Head Teacher

Dated: April 2018