

The Good Shepherd Multi Academy Trust

Data Protection policy



**The Good Shepherd
Multi Academy Trust**

Review January 2017

Values

Every member of the Trust family of schools will be valued and encouraged to fulfil their potential. In our Trust we believe:

- Everyone has something to offer
- Trust, honesty, empathy and social responsibility are the Christian values that frame our work
- We are here for the whole person, spiritually, morally, educationally and socially
- In working with transparency and openness

The Good Shepherd Multi Academy Trust: Data Protection Policy

1. Introduction

- 1.1 This document is a statement of the aims and principles of the Trust, for ensuring the appropriate handling of personal and sensitive information relating to staff, pupils, parents and governors.

This policy takes due note of the information and guidance published by the Information Commissioners Office

(http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx)

It is the responsibility of the Trust to ensure registration with the ICO is undertaken.

Aims

- To comply fully with the requirements of the Data Protection Act 1998.
 - To ensure that all processing is appropriately registered / notified and review and update notified entries.
 - To ensure that all staff involved with the collection, processing and disclosure of personal data are made aware of their duties and responsibilities within these guidelines.
- 1.2 The Good Shepherd MAT is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. Personal information or data is defined as data which relates to a living individual who can be identified from that data or other information held.
- 1.3 All schools in the Trust needs to keep certain information about our employees, pupils and other users to allow us, for example, to monitor performance, achievement, and health and safety.

- 1.4 To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Trust and its school must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).
- 1.5 In summary these principles state that personal data shall:
- i. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
 - ii. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
 - iii. Be adequate, relevant and not excessive for that purpose.
 - iv. Be accurate and kept up to date.
 - v. Not be kept for longer than is necessary for that purpose.
 - vi. Be processed in accordance with the data subject's rights.
 - vii. Be kept safe from unauthorised access, accidental loss or destruction.
- 1.6 All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2. The Data Controller and the Designated Data Controllers

- 2.1 The Academy Trust as the corporate body is the Data Controller under the 1998 Act, and the Directors are therefore ultimately responsible for implementation. A nominated director (**Academic year 15/16: Patrick Freeman**) is the Designate Data Controller for the Trust.

However, the Designated Data Controllers in each Academy (school) will deal with day to day matters.

- 2.2 Each school has two Designated Data Controllers: They are the
- Headteacher and the Senior Member of the Office staff (school business manager).
- 2.3 Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

3. Responsibilities of Staff

3.1 All staff are responsible for:

- i. Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- ii. Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
- iii. Handling all personal data (eg – pupil attainment data) with reference to this policy, the school's confidentiality policy and the guidelines in the staff handbook.

4. Data Security

4.1 All staff are responsible for ensuring that:

- i. Any personal data that they hold is kept securely.
- ii. Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

4.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

4.3 Personal information should:

- i. Be kept in a locked filing cabinet, drawer, or safe; or
- ii. If it is computerised, be encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- iii. If a copy is kept on a usb memory key or other removable storage media, that media must itself be encrypted/password protected and/or kept in a locked filing cabinet, drawer, or safe.

5. Rights to Access Information

5.1 All staff, parents and other users are entitled to:

- i. Know what information the School holds and processes about them or their child and why.
- ii. Know how to gain access to it.
- iii. Know how to keep it up to date.

iv. Know what the School is doing to comply with its obligations under the 1998 Act.

5.2 The School will, upon **written** request (to the designated data controller / protection officer), provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

5.3 All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Designated Data Controller.

5.4 The School may make a charge on each occasion that access is requested, although the School has discretion to waive this. (Normally £10 for each request)

5.5 The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

6. Exempt Information

6.1 The Data Protection Act 1998 allows exemptions as to the provision of some information therefore all information will be reviewed prior to disclosure. Third party information provided by someone else such as another child, parent, Police, Local Authority, Health Care professionals or another school will need their consent before it can be disclosed.

6.2 Likewise any information which may cause serious harm to the physical, mental or emotional wellbeing of the pupil or any another person should not be disclosed, nor should information that would reveal that the child is at risk of abuse or information relating to court proceedings.

6.3 Where redaction has taken place (information blacked out/removed) a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

7. Retention of Data

7.1 The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references.

7.2 Different categories of data will be retained for different periods of time.

- 7.3 Out of date data/information will be discarded if no longer relevant. Personal data will only be kept as long as reasonably needed, for legal or business purposes.

8. Monitoring and Evaluation

- 8.1 This policy will be reviewed annually, or if there are changes to relevant legislation