Communitas
Education Trust

Data Protection Policy (GDPR) - Draft

Created: May 2018

Last update: May 2018

Review by: June 2019

CONTENTS

1. **Introduction**
2. **Purpose of Policy**
3. **What is Personal Information?**
4. **Categories of Personal Information**
5. **Roles and Responsibilities**
6. **Collecting Personal Information**
7. **Privacy Notices**
8. **General Handling of Personal Information**
9. **Sharing of Personal Information**
10. **Requests for Information (SAR,FOI)**
11. **Data Breaches**
12. **Training**
13. **Data Protection Impact Assessments**
14. **Review**

Appendices

A. **Overview of Data protection Documents**
B. **Data Retention Schedule**
C. **Data Breach Procedures**
D. **Requests for information**
E. **Staff Acceptable Use Policy**
F. **Digital Storage Protocols**
G. **Non Disclosure Agreements**
H. **Data Protection Impact Assessment**

Introduction

Schools within the Communitas Education Trust collect and use personal information about staff, students, parents or carers and other individuals who come into contact with the schools. This information is gathered in the process of providing educational and other associated services. In addition, there may be a legal requirement to collect and use information to ensure that the schools comply with their statutory obligations.

In collecting, processing, sharing and disposing of personal information relating to living individuals, school's within the Trust are bound by the General Data Protection Regulation 2016.

The Information Commissioner's Office enforces the Regulation, issues relevant guidance and registers personal data sets held by any organisation.

As a data controller, each School must register itself with the Information Commissioners Office (ICO) annually.

This document sets out the Trusts policy for compliance with the General Data Protection Regulation (GDPR).

Purpose

The objective of this policy is to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation 2016, and other related legislation. It will apply to all personal information that is collected, used, recorded, stored and applies to both paper and electronic files.

All staff involved with the collection, processing and disclosure of personal information will be aware of their duties and responsibilities set out in this policy.

What is Personal Information?

Personal information is defined as data which relates to a living individual, identifiable from that information.

The Six Guiding Principles

The General Data Protection Regulation 2016 establishes six enforceable principles and School's name as a registered Data Controller under the Act, will comply with these principles below:

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Act creates a single framework for access to personal information about living individuals held in both paper and electronic form.
See guidance on what to do when a Subject Access Request (SAR) is received in Appendix D - Requests for Information.

Categories of Personal Information

Personal information refers to any information, held manually or electronically, which relates directly to a living individual.

Personal information can include but is not limited to:

- Name and Address
- Contact Number
- E-mail address
- Date of Birth

Special categories of information includes information under the following headings:

- Race or ethnic origin
- Political opinion/s
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Genetic and Biometric data
- The commission or alleged commission of offences, court sentences or allegations under investigation

While not legally special category of data, the following should be given special consideration whilst processing:

- Qualifications
- Income level
- Employment history
- Bank Details

Roles and Responsibilities

ALL STAFF

- All staff have a responsibility to abide by the principles of the Data Protection Act. Staff should be aware of the policy and adhere to the guidelines to ensure that information is handled appropriately. Any breach of this policy could lead to disciplinary action being taken.

AGENCY STAFF AND CONTRACTORS

- The Trust expects all agency staff and contractors to adhere to this policy and guidance. Agency staff and contractors should be provided with a copy of this policy prior to accessing personal information as part of their role. In addition, a non disclosure agreement (Appendix G) should be signed before accessing personal information.

DATA PROTECTION OFFICER (DPO AS A SERVICE)

- Must be in a position to undertake their tasks independently and will report directly to the Head Teacher and Trust CEO
- Be a point of contact for data protection issues
- Be involved in a timely manner in all data protection issues
- Respond to requests for access to personal data within 30 calendar days
- Inform and advise the school, processors and employees of obligations
- Monitor data protection compliance
- Advise as required on Data Protection Impact Assessments
- To co-operate with supervisory authority, Information Commissioner's Authority (ICO)
- To act as contact point for the supervisory authority (ICO)
- Have due regard to the risk associated with processing, taking account of nature, scope and context of processing.

HEAD TEACHER & SCHOOL BUSINESS MANAGER/DATA MANAGER

- Provide guidance to ensure all staff are aware of their data protection responsibilities under the act
- Responsible for managing and reporting data breaches to the trusts data protection officer
- Providing guidance to process Subject Access Requests and Freedom of Information requests
- Maintain an overview of school data eco system and update data protection documents
- Ensure an up-to date information sharing agreement is in place with all third party organisations and a record of this has been made.
- Ensuring appropriate and adequate training is undertaken by staff
- Ensuring staff are compliant with this policy and any associated procedures

SCHOOL DESIGNATED DP STAFF

- Handle requests to share personal information from third parties.
- Make a considered decision on the appropriate data to share, and ensure this process is carried out securely, with the minimum level of personal information to fulfil the obligation or provide the service.

Collecting Personal Information

The data protection act requires all data controllers to process personal and sensitive data fairly and lawfully.

Only designated school DP staff should be involved in the collection of personal information.

When collecting personal and/or sensitive information from individuals, it is important that they understand who we are and the purpose for which their information is being collected. Schools should ensure that parents/guardians are provided with the school's privacy notice when a child first starts at the school. A staff specific privacy notice should also be provided to staff when they begin employment with the school.

Some personal and/or sensitive information will be collected throughout a pupil or member of staff's time at the school. This information will be kept securely at all times and could be subject to any 'Access to Information' requests. Information should only be retained in line with retention periods outlined in the Trusts data retention schedule (Appendix B) and holding it indefinitely could result in a data breach.

Privacy Notices

The Trust is committed to processing personal data fairly and lawfully and have a privacy notice visible and easily accessible on the Trust and each school's website explaining how data will be used. Individuals will be able to read the statement before completing a data collection form (paper or electronic), and will know exactly why the data is being collected and for what specific purpose/s.

The privacy notice should be provided to the individual, or the parent/guardian of the pupil when the information is obtained from the individual

The Trust has provided a privacy notice template, however it is the Schools responsibility to ensure their privacy notice tells individuals the following about the school:

- Name of the school
- The school address and contact details
- What we are going to use their data for and legal basis for doing so
- Who we will share individual's data with
- Individuals rights to accessing their own information, including the fact that the data subject can complain to The Information Commissioner
- How we will keep individuals data secure and protected
- Identity & contact details of the Trusts Data Protection Officer
- The retention period for the data
- Any legal or contractual requirement to provide the information to other government agency, including law enforcement
- Automated decision making, with information about the consequences.

A privacy notice should be informative and clear enough for children to understand and provide reassurance that the school will handle personal data appropriately.

General Handling of Personal Data

The Trust is committed to keeping personal information secure at all times. The Trust promotes a just in time policy for accessing personal data and a clear screen and desk policy. This is detailed in the staff Acceptable Use and digital storage protocols documents.

The Trust expects all staff to adhere to the following when handling personal data:

- Treat all personal information with equal respect for confidentiality and security whether in written, spoken or electronic form.
- Ensure that personal information is kept secure at all times, including paper copies.
- The majority of personal information should be stored electronically on the schools IT and MIS systems (including 3rd party software)
- Personal information should only be accessed by school staff to accomplish a specific task and where practical, this should be done within the schools IT systems
- Staff should avoid making hard copies of personal information, unless it is absolutely necessary
- If hard copies are necessary for a particular purpose; the hard copies should be securely stored in a locked filing cabinet and shredded using the schools cross cut shredders as soon as the purpose has been fulfilled
- Documents and reports containing personal information about staff or students that have been provided to the school by outside agencies/ third parties should be attached to the child or staff record within the MIS. School staff that need access to the document or report should do so within the school MIS system.

Sharing of Personal Data

The Trust understands that people must feel confident that their personal information is kept safe and secure, and that schools maintain the privacy of the individual whilst sharing information to fulfil its obligations and provide services. It is therefore important that the school can share information appropriately as part of their day-to-day practice while protecting this information.

Only designated school DP staff are authorised to share information with third party organisations. School DP staff will receive additional training to ensure they are able to share information safely and proportionately. This will include, but is not limited to: office staff, headteachers, deputy headteachers, designated safeguarding leads, Special Education Needs staff, pastoral staff and IT staff.

The information that is provided to third party organisations must be the minimum necessary to fulfil the legal obligation or to enable the third party to provide a service.

Third Party organisations working with schools must provide and follow information sharing agreements set out when sharing information. These agreements detail information about data including obtaining, storing, recording, disposal and sharing of information between the school and third parties. This Information will be recorded by the school, and it is the schools responsibility to ensure an uptodate information sharing agreement is in place with all third party organisations.

Requests for Information (SAR,FOI)

SUBJECT ACCESS REQUESTS (SARS)

Individuals have the right to ask for access to their information which can include factual information, expressions of opinion, and the intentions of the school in relation to them, irrespective of when the information was recorded.

There are two distinct rights of access to the information schools hold about pupils:

- **Right to the educational record**
  Under the Education (Pupil Information) (England) Regulations 2005, a parent or legal guardian has the right to access their child's educational record.
- **Subject access requests**
  Under the General Data Protection Regulation 2016, a pupil has a right to see their own information. A parent or legal guardian may also make a request on behalf of their child.

If a pupil or parent makes a request for educational records, the school must respond within 15 school days. Fees for these requests will depend on the number of pages of information supplied.

If a pupil or parent makes a subject access request for personal information, the school must respond promptly and at most within 30 calendar days. All subject access requests should be made to the Trust DPO who will oversee the process of fulfilling the request. Schools will be unable to charge for most Subject Access Requests

See Appendix D Requests for information for more details.

FREEDOM OF INFORMATION REQUESTS (FOI'S)

The Freedom of Information Act 2000 (FOIA) provides public access to information held by schools. It does this in two ways: schools are obliged to publish certain information about their activities; and members of the public are entitled to request information from schools.

The Trust and its schools will comply with Freedom of Information requests and release non personal and non confidential information held by the school, after applying any relevant exemptions to protect certain categories of information.

The Act requires that all requests must be in writing (to include letters, faxes and e-mails). Requests must state clearly what information is required and must provide the name of the person with an address for correspondence.

On receipt of a FOI request, the school must respond promptly and in any event within 20 working days.

See Appendix D Requests for information for more details.

Data Breaches

The following are examples of data breaches and not limited to;

- Reading confidential files when there is no requirement to do so
- Giving excessive/unnecessary information
- Sending information in error eg. to a wrong email address
- Files/records removed from the office or lost
- Unencrypted devices used and lost containing personal/sensitive details
- Information that hasn't been redacted correctly before publishing

Known breaches in confidentiality must be reported to the DPO immediately so it can be recorded and a formal investigation carried out.

The DPO will follow the Data Breach Process - see appendix C

Training

Schools will arrange training for all staff so they are fully aware of their obligations and responsibilities under the Data Protection Act. Training will be appropriate to the individual roles of staff with additional training given to staff who, as part of their role process or share personal data on a regular basis. This will include, but is not limited to: office staff, headteachers, deputy headteachers, designated safeguarding leads, Special Education Needs staff, pastoral staff and IT staff.

Data Protection Impact Assessments

A data protection impact assessment (appendix H) should be conducted when a school within the Trust implements a new system, or a significant change to an existing system involving personal data; the impact assessment should be conducted by IT staff member and/or the school business manager/data manager and should then be sent to the DPO for approval, to ensure that the new system is compliant and that data protection has been considered.

Review

This policy will be reviewed annually. Next review date will be in May 2019.