
# DATA PROTECTION POLICY

September 2019

# DOCUMENT CONTROL

| | | |
|---|---|---|
| Author/Contact | Sarah Harrington<br>Tel: 01622 743286 ext. 212<br>sarah.harrington@futureschoolstrust.com | |
| Document Reference | Data Protection Policy | |
| Version | 03 | |
| Status | Approved | |
| Publication Date | September 2019 | |
| Related Policies | Freedom of Information Policy<br>CCTV Policy | |
| Review Date | September 2021 | |
| Approved/Ratified by | Resources Committee | Date: September 2019 |
| Distribution: Future Schools Trust Staff<br>Please note that the version of this document contained within the VLE is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments. | | |

## POLICY STATEMENT

Future Schools Trust (FST) is required to process relevant personal data regarding staff, students, their parents and carers has the legal right and a legitimate interest to collect and process personal data relating to those we employ to work within the Trust, or those otherwise contracted to work with us for public interest. We shall take all reasonable steps to do so in accordance with this policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. Reference to students in this policy includes current, past or prospective students. Please refer to the academy's Freedom of Information Policy which supplements this policy.

FST is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

**CONTENTS**

## 1. INTRODUCTION

Future Schools Trust needs to keep certain information about our employees, pupils and other users to allow us to monitor performance, achievement, and health and safety. 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, we must comply with the Data Protection Principles which are set out in the General Data Protection Regulation (GDPR).

In summary these principles state that personal data shall:

- Be obtained and processed fairly and lawfully
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for that purpose
- Be accurate and kept up to date
- Not be kept for longer than is necessary for that purpose
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to other countries without adequate protection

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 Trust 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 Trust. Any failures to follow the policy can therefore result in disciplinary proceedings.

## 2. DEFINITIONS

**Personal Data**

Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'personal data' is information which relates to a living, identifiable individual.

In the context of this document and the Trust's requirement to process personal data as part of its duty of care and to educate its students, personal data may include:

- school admission and attendance registers
- students' curricular records
- reports to parents/carer on the achievements of their children
- records in connection with students entered for prescribed public examinations
- staff records, including payroll records and personnel records
- student disciplinary records
- personal information for teaching purposes
- records of contractors and suppliers

**Sensitive Personal Data**

Sensitive Personal data may include:

- ethnic or racial origin
- languages and religious beliefs
- other beliefs of a similar nature
- membership of a trade union
- medical and mental health information
- details of any criminal offence(s) or alleged offence(s) committed
- Sexual orientation
- SEN information/curriculum assessments

Where sensitive personal data is processed by the Trust, the explicit consent of the appropriate individual will be requested in writing.

## 3. PROCESSING PERSONAL DATA

If it is necessary for the Trust to process certain personal data to fulfil its obligations to staff, students and their parents or guardians, then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt, will remain confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

The Trust may only process a member of Staff's Personal Data if the Data Subject consents or if the processing is necessary to any of the following:

1. The performance of a contract to which the Data Subject is a party or for taking steps at their request to enter into a contract
2. Compliance with any legal obligation (other than a contractual obligation) to which the Data Controller is subject
3. To protect the vital interests of the Data Subject
4. For the administration of justice or the exercise of any functions conferred on any person by or under any enactment
5. For the purposes of legitimate interests pursued by the Data Controller or by third parties to whom Data is disclosed provided it would not prejudice the rights and freedoms or legitimate interests of the Data Subject.

The School may only process Sensitive Personal Data if, in the following circumstances:

1. The Trust would be entitled to process Personal Data and
2. Either:
   a) the Data Subject has given his or her *explicit* consent to processing or
   b) any of the following circumstances apply:
      i) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust by law in connection with the Data Subject's employment. This may include but is not limited to dealing with sickness absence, dealing with disability and making adjustments for the same
      ii) The processing is necessary in relation to legal rights, advice or proceedings. This may include but is not limited to obtaining legal advice, establishing or exercising or defending legal rights or the conduct of any legal proceedings (including prospective legal proceedings)
      iii) The processing is necessary to trace equality of opportunity between people of different racial or ethnic backgrounds

The School will process Sensitive Personal Data for legal, personnel, administrative and management purposes including but not limited to processing:

- information about a member of Staff's physical or mental health or condition in order to monitor sick leave and take decisions as to their fitness for work
- the member of Staff's racial or ethnic origin or religious or similar beliefs, age and sexual orientation, political beliefs and sexual life in order to monitor compliance with equal opportunities legislation and to carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements from time to time in force
- information relating to the commission or alleged commission of any criminal offence for insurance purposes and in order to comply with legal requirements and obligations to third parties
- information relating to any criminal proceedings in which the member of Staff has been involved for insurance purposes and in order to comply with legal requirements and obligations to third parties
- information relating to the any member of Staff's union membership for the purposes of administering collective or individual consultations of managing any internal procedures at which staff have the right to be accompanied by a trade union representative

The following principles shall apply whenever Sensitive Personal Data is handled or processed by the Trust:

- The information to be obtained and processed will be obtained and processed fairly and lawfully
- No member of Staff shall be knowingly deceived or misled as to the purposes for which the information has been obtained or processed

- The Trust shall wherever reasonably practicable, advise the Data Subject of any information it intends to retain, the purpose of processing and any further information necessary for the processing of that data to be fair
- Information will only be obtained or processed for one or more specified and lawful purposes
- Information held on a Data Subject should be adequate, relevant and not excessive in relation to the specified purpose for which it has been obtained or processed
- Information shall be accurate and where necessary will be kept up to date
- No information will be kept for longer than is necessary to satisfy the purpose for which it was originally obtained or processed
- All information must be protected against unauthorised processing or damage. The level of security shall be appropriate to the nature of the data and the harm which could result from misuse
- No information will be exported outside the EEA unless it is to a country where the rights of the Data Subject can be adequately protected

## 4. DATA CONTROLLERS AND DATA PROTECTION OFFICERS

The Trust, as a body, is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Protection Officers will deal with day to day matters.

The Trust has identified its Designated Data Controllers as the CEO, the Headteachers, ICT & Facilities Manager and HR Manager. The Trust also has designated Data Protection Officers, please contact Sarah Harrington, HR Manager for further information.

## 5. RESPONSIBILITIES OF STAFF

All staff are responsible for:

1. Checking that any information that they provide to the Trust in connection with their employment is accurate and up to date
2. 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 Headteacher cannot be held responsible for any errors unless the staff member has informed the Trust of such changes
3. Handling all personal data (e.g. – pupil attainment data) with reference to this policy.

## 6. DATA SECURITY

Where it is reasonably practicable, the School will take steps to ensure that members of staff will only have access to personal data relating to students, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties under the GDPR. The School will ensure that all personal information is held in a secure central location and is not accessible to unauthorised persons.

Staff should not use memory sticks and use the cloud based system as this provides a higher level of security and reduces the risk of data protection breaches.
All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely
- 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
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases

Personal information should:

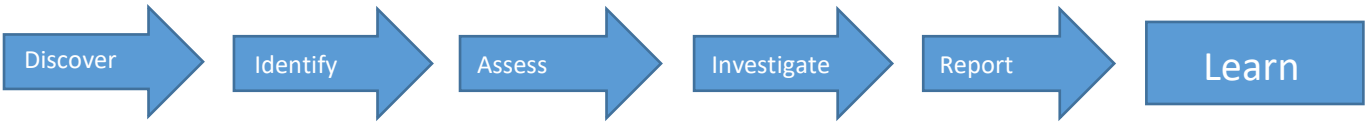
- Be kept in a filing cabinet, drawer, or safe in a secure office
- If it is computerised, be password protected both on a local hard drive and on a network drive that is regularly backed up
- Not be kept on a USB memory key or other removable storage media

## 7. DATA BREACHES

A data protection breach is the result of an event or series of events where personal information is or could be exposed to unauthorised or inappropriate processing that results in the security being compromised. Examples of common incidents are as follows:

| Type | Example |
|---|---|
| Technical | Data Corruption<br>Malware<br>Hacking |
| Physical | Unescorted visitors in secure areas<br>Break-ins<br>Theft |
| Human Error | Data input error<br>Non-secure disposal of data<br>Unauthorised disclosures |

If a breach in data protection is detected, the individual should notify their Data Protection Officer as a matter of urgency outlining the details of the breach. Those involved in the data breach will be expected to liaise with the Data Protection Officer in order to minimise any further damage in the first instance and to notify those who are affected by the breach. The following breach tool should be followed:




Once the discovery has been reported to the Data Protection Officer and the breach identified, the damage or potential damage should be assessed and a formal investigation begun. This is achieved by interviewing key personnel involved in the breach and their line managers and collecting as much information as possible to determine how the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified. The objective of any breach investigation is to identify what actions the Trust needs to take to first prevent a recurrence of the incident and second to determine whether the incident needs to be reported to the Information Commissioner's Office. The purpose of the report is to document the circumstances of the breach, what actions have been taken and what recommendations have been made and whether the disciplinary process needs to be followed.

Not all data protection breaches will result in formal action. Some will be false alarms or 'near miss' events that will not cause immediate harm to individuals or the Trust. These should still be reported, as analysis of these will allowed lessons to be learnt and continual improvement.

## 8. RIGHTS TO INFORMATION

Under the GDPR, the rights to the data belong to the individual to whom the data relates. However, in most cases, the Trust will rely on parental consent to process data relating to students unless, given the circumstances and the student's age and understanding, it is unreasonable to rely on the parent's consent. Parents should be aware that in such situations they may not be consulted. These situations are very rare, and it is a general policy in the Trust to always seek parental or guardian consent before processing a child's personal data.

An individual has the following rights to their information:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure

- The right to restrict processing
- The right to data portability
- The right to withdraw consent to holding sensitive personal data
- Rights in relation to automated decision making and profiling

Individuals have a right of access to information held by the School. Any individual wishing to access their personal data should put their written request to the Headteacher through a Subject Access Request. The Trust/Academy will try to respond to any such written requests as soon as is reasonably practicable and in any event, within the time compliance requirements of the GDPR.

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the School is doing to comply with its obligations under the GDPR

The Trust will provide all staff and parents and other relevant users with a statement regarding the personal data held about them in the form of a privacy notice. This will state all the types of data the Trust holds and processes about them, and the reasons for which they are processed.

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 Headteacher. The Trust will ask to see evidence of your identity, such as your passport or driving licence, before any disclosure of information is made.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, as required by the GDPR.

It is important to note that certain data is exempt from the right of access under the GDPR. This can include:

- information which identifies other individuals
- information which the Trust reasonably believes is likely to cause damage or distress
- information which is subject to legal professional privilege
- student examination scripts

## 9. RETENTION OF DATA

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

| File | Retention Period | Action |
|---|---|---|
| All records leading to an unsuccessful school admission and appealed | Resolution of case + 1 year | Secure Disposal |
| All records leading to an unsuccessful staff appointment | Date of appointment of successful candidate + 6 months | Secure Disposal |
| Students Records (Primary) | Whilst the student is enrolled | Secure Disposal |
| Student Records (Secondary) | Date of Birth of student + 25 years | Secure Disposal |
| Staff Employment File | Employment end date + 6 years | Secure Disposal |
| Staff Discipline Warnings | Variable – see Disciplinary policy | Secure Disposal |

## 10. ACCURACY

In accordance with the GDPR it is Trust policy to ensure that any personal data held about an individual is accurate. Conversely, it is encouraged that all students and staff to notify the School/Trust of any changes to information held about them (change of address, change of marital status etc.).

## 11. ENFORCEMENT

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the GDPR, they should make a complaint to the School using the School's Complaints Procedure.

## 12. COMPLAINTS

The Information Commissioner is responsible for monitoring and enforcing the GDPR, and he / she can investigate, where necessary issue an advisory or enforcement notice, and in some cases prosecute. The Information Commissioner requires that complaints are first brought to the attention of Future Schools Trust, to provide an opportunity for investigation and solution.

Any complaints follow the Trust's complaints procedure. If the complainant is still not satisfied, they should be referred to the Information Commissioner's Office.