



# Data Protection Policy

## All Trust Staff

<b>DISTRIBUTION</b>	This is a Trust-wide policy and applies to all staff within the Trust.		
<b>DOCUMENT ID</b>	FT-IT005 Data Protection Policy		
<b>AUTHOR</b>	HRS	<b>VERSION</b>	1.1
<b>RATIFIED BY THE DIRECTORS OF THE FALLIBROOME TRUST</b>			
<b>POLICY REVIEW CYCLE</b>	2 YEARS		
<b>POLICY REQUIREMENT</b>	STATUTORY		

The Fallibroome Trust, Priory Lane, Macclesfield, Cheshire, SK10 4AF  
Telephone: +44 (0) 1625 827 898 | Email: [info@fallibroometrust.org.uk](mailto:info@fallibroometrust.org.uk) | Web: [www.fallibroometrust.org.uk](http://www.fallibroometrust.org.uk)

The Fallibroome Trust (Company number: 07346144). A company incorporated as private limited by guarantee.  
Registered Office situated in England and Wales

# CONTENTS

Introduction.....	3
Purpose .....	3
Governance .....	3
Scope.....	3
Data protection officer (DPO).....	4
Data protection principles .....	5
Cloud services .....	5
Fallibroome Trust practice .....	6
Appendix 1: Secure Data Handling .....	8
Step 1 .....	8
Step 2 .....	8
Step 3 .....	9
Appendix 2: Dealing with a subject access request.....	10
Appendix 3: Sample Subject Access Request Letter and Form .....	12

# INTRODUCTION

At the Fallibroome Trust, we acknowledge that to function properly we need to collect and use certain types of information about staff, students and other individuals who encounter the Fallibroome Trust. We are also obliged to collect and use data to fulfil our obligations to the local authority (LA), DFE and other bodies.

We deal with information properly in whatever way it is collected, recorded, and used – on paper, electronically, in the ‘cloud’ or any other way. We regard the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We are conscious that much of the data we hold is classified as sensitive personal data and we are aware of the extra care this kind of information requires.

We ensure that our organisation treats all personal information lawfully and correctly. To this end, we fully endorse and adhere to the data protection principles as contained in the Data Protection Act.

## PURPOSE

This policy aims to:

- Outline the procedure and protocols to adhere to for compliance of the Data Protection Act, this includes the UK’s implementation of the General Data Protection Regulation (GDPR)

## GOVERNANCE

The Local Governing Body is a committee of the Fallibroome Trust. The Local Governing Body will adopt and comply with all policies communicated by the Directors of the Trust. The Local Governing Body is responsible for setting out the policies and practices for staff. The Local Governing Body may delegate these matters to:

- The Principal/Head teacher;
- A sub-committee of the Local Governing Body; or
- A sub-committee and the Principal/Head teacher.

Where this procedure refers to the Local Governing Body representative this can be any one of the above.

## SCOPE

This procedure applies to all employees (including governors and volunteers) of the Fallibroome Trust.

# DATA PROTECTION OFFICER (DPO)

The Fallibroome Trusts data protection officer is:

James England, Data Protection Education.

1 Saltmore Farm, New Inn Rd, Hinxworth, Baldock, SG7 5EZ.

Telephone: 0800 0862018

Email: [dpo@dataprotection.education](mailto:dpo@dataprotection.education)

# DATA PROTECTION PRINCIPLES

All members of staff employed in the Fallibroome Trust are required to adhere to the eight enforceable data protection principles as set out in the current Data Protection Act. Data shall be processed fairly and lawfully and shall not be processed unless specific conditions are met.

- Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects under the current Data Protection Act
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data whether it is held internally, or cloud based
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

There is stronger legal protection for more sensitive information such as:

- Ethnicity
- Background
- Political opinions
- Religious beliefs
- Health
- Sexual health
- Criminal records

## CLOUD SERVICES

We as the Fallibroome Trust are responsible for:

- Ensuring that the processing carried out by our cloud service provider complies with the DPA requirements by means of a contract and data processing agreement.
- Ensuring the accuracy of the self-certification statements made by the cloud services suppliers by using the self-certification checklists facilitated by the DFE.

# FALLIBROOME TRUST PRACTICE

Within the Fallibroome Trust, we will strictly apply the following criteria and controls. These are to:

- Notify the Information Commissions Office (ICO) that we process personal data and re-notify if procedures change or are amended
- Observe fully the conditions regarding the fair collection and use of information. To achieve this, we have in place and use a privacy notice, sometimes called a fair processing notice
- Meet our legal obligations to specify the purposes for which information is used
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply strict checks to determine the length of time information is held
- Ensure that the rights of the persons about whom information is held can be fully exercised under the legislation. These include the right to be informed that processing is being undertaken, the right to access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information, which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information. We will review the physical security of buildings and storage systems as well as access to them. All portable electronic devices must be kept as securely as possible on and off Fallibroome Trust premises
- Ensure that all Disclosure and Barring Service (DBS, formerly Criminal Records Bureau) records (recruitment and vetting checks) are kept in a safe central place and that no unnecessary certification information is kept longer than six months
- Ensure that personal information is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation, or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information – see appendix 1
- Have in place secure methods for safely disposing of all electronic and paper records
- Ensure that photographs of pupils are not included in any Fallibroome Trust publication or on the a Fallibroome Trust website without specific consent
- Ensure that biometric data concerning pupils are not obtained or used without the knowledge of the child and parents and without permission being obtained from them as appropriate
- Take care that CCTV that captures or processes images of identifiable individuals is done in line with the data protection principles

The Fallibroome Trust shall also ensure that:

- There is a named person with specific responsibility for data protection within the Fallibroome Trust (see data protection officer)
- All persons managing and handling personal information understand that they are contractually responsible for following good data protection practice
- All persons managing and handling personal information are trained to do so
- Anyone wanting to make enquiries about handling personal information knows what to do
- Anyone managing and handling personal information is appropriately supervised
- Queries about handling personal information are properly and courteously dealt with
- Methods of handling personal information are clearly described
- A regular review and audit is made of the way personal information is held, managed and used
- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated
- A breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned
- On occasions when information is authorised for disposal, it is done appropriately

# APPENDIX 1: SECURE DATA HANDLING

In deciding the most appropriate way to share information and the level of security required, always take into consideration the nature of the information and the urgency of the situation, that is, take a risk-based approach to determining appropriate measures. The simplified process described below will help members of staff and the Trust itself choose the appropriate level of security needed when sharing potentially sensitive information. The data protection officer (DPO) is responsible for ensuring that staff are trained to use this process.

## STEP 1

Imagine a potential security breach e.g., a confidential letter is left in a public area, a memory stick is lost, or someone reads information on a computer screen while waiting to meet a member of staff, and consider:

- Will it affect or identify any member of the Trust, school, or community?
- Will someone lose/be out of pocket by more than £100?
- Will it cause any kind of criminal case to fail?
- Is there a risk of discomfort/slur upon professional character of someone?
- Is anyone's personal safety at risk?
- Will it embarrass anyone?

If the answer to all the above questions is 'no', the document does not contain sensitive information. If the answer is 'yes' to any of the questions above, then the document will include some sensitive information and therefore requires a level of protection.

## STEP 2

Imagine the same potential security breach as above, and consider:

- Will it affect many members of the school or local community and need extra resources locally to manage it?
- Will an individual or someone who does business with the school lose/be out of pocket by £1,000 to £10,000?
- Will a serious criminal case or prosecution fail?
- Is someone's personal safety at a moderate risk?
- Will someone lose his or her professional reputation?
- Will a company or organisation that works with the school lose £100,000 to £1,000,000?

If the answer to any of the above questions is 'yes' then the document contains sensitive information and additional security should be considered, such as password protecting and encrypting the document before it is emailed to a colleague outside of the school or Trust.

However, if you think that the potential impact exceeds that stated in the question (e.g. someone's personal safety is at high risk) think very carefully before you release this information at all.



## STEP 3

All documents that do not fit into steps 1 or 2 might require a higher level of protection/security if released at all. Err on the side of caution and seek guidance from the relevant line manager/senior member of staff.

## APPENDIX 2: DEALING WITH A SUBJECT ACCESS REQUEST

- Requests for information must be made in writing (which includes the use of e-mail) and be addressed to the principal / head teacher. If the initial request does not clearly specify the information required, then the Fallibroome Trust will make further enquiries. Appendix 3 contains a sample letter and form that may be used to request further information, or as a template for the initial request
- The principal / head teacher must be confident of the identity of the individual making the request. When the request concerns data about a pupil, checks will also be carried out regarding proof of relationship to the child. In addition, evidence of identity will be established by requesting one of the following:
  - Passport.
  - Driving licence.
  - Utility bills with the current address.
  - Birth/marriage certificate.
  - P45/P60.
  - Credit card or mortgage statement (this list is not exhaustive).
- As stated above, any individual has the right of access to information held about them. However, in the case of children this is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request. The principal / head teacher should discuss the request with the child and consider their views when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child.
- The response time for subject access requests, other than for educational records, is 1 month from receipt (this refers to calendar days irrespective of Fallibroome Trust holiday periods).
- The current DPA allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.
- Third party information is information that has been provided by another person such as the LA, the police, a health care professional or another school. It is normal good practice to seek the consent of the third party before disclosing information. Even if the third party does not consent, or consent is explicitly not given, the data may be disclosed. (There is no need in the case of third party requests to adhere to the 40-day/one-month statutory timescale.)
- Any information that could cause serious harm to the physical, emotional or mental health of a pupil or another person may not be disclosed, nor should information that would reveal that the child is at risk of abuse. The same stricture applies to information relating to court proceedings.
- If there are concerns about the disclosure of information, then additional advice should be sought, usually from the Information Commission's Office.
- When redaction (blacking out or obscuring of data) has taken place, then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

- Information disclosed should be clear, with any codes, technical terms, abbreviations or acronyms explained. If information contained within the disclosure is difficult to read or illegible, it will be retyped.
- Information can be provided at the local school with a member of staff on hand to assist if requested, or provided at face-to-face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used, then registered or recorded mail will be used.
- Complaints will be dealt with in accordance with the Fallibroome Trust complaints procedure, which is available on-line or from the Fallibroome Trust office. Should the complainant wish to take the matter further, it may be referred to the Information Commissioner <https://ico.org.uk>.
- This policy will be reviewed by the Fallibroome Trust at least every two years.

# APPENDIX 3: SAMPLE SUBJECT ACCESS REQUEST LETTER AND FORM

*Insert the Schools name and address*

**Re: subject access request**

FAO: The Fallibroome Trusts Data Protection Officer,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer  Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: <i>Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:</i> <ul style="list-style-type: none"> <li>• <i>Your personnel file</i></li> <li>• <i>Your child's medical records</i></li> <li>• <i>Your child's behavior record, held by [insert class teacher]</i></li> <li>• <i>Emails between 'A' and 'B' between [date]</i></li> </ul>

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a fee to provide this information, and in most cases, you must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely,

*Requesters Name*