

Data Protection Policy



St John Fisher Catholic Voluntary Academy

Mission Statement

This Mission Statement reflects the views of our pupils, staff and parents

'For I know the plans I have for you; plans to give you hope and a future.' Jeremiah 29:11

- I know that God made me and that he loves me very much.
- I want to grow in God's love and be the best that I can be.
- Every day I will get to know God better in prayer and meditation.
- I will always follow the academy rules because I know that they are there to help me and to make this a happy academy where children can learn.
- I will show care and respect for everyone I meet at all times.
- I will always try my best, even when I find things difficult.
- I will come to academy every day unless I am really too ill to attend.
- I will always tell the truth, even if I have done wrong.
- I will take care of the academy building, grounds and everything in it.
- My parents and everyone who works at Saint John Fisher will work together and always try their best to help me make the most of my God-given talents.

Data Protection Policy

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

St John Fisher CVA intends to comply fully with the requirements and principles of the Data Protection Act 1998.

We have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

St John Fisher CVA collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. 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. This information is gathered in order to enable it to provide education and other associated functions.

In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. We also have a duty to issue a Privacy Notice to all pupils, parents and staff; this summarises the information we hold, why it is held and the other parties to whom it may be passed on.

1. Scope of the Policy

This policy is intended to ensure that personal information held by St John Fisher CVA is dealt with correctly and securely and in accordance with the Data Protection Act 1998 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing, disclosure and destruction of personal data will be aware of their duties and responsibilities by adhering to these guidelines

Pupils, parents and staff have the right to access information held by the school. The most important rights are contained in the following legislation:

- Data Protection Act 1998 <http://www.legislation.gov.uk/ukpga/1998/29/contents>
- Education (Pupil Information) (England) Regulations 2005
- Freedom of Information Act 2000
<http://www.legislation.gov.uk/ukpga/2000/36/contents?text=primary%20schools#match-1>

2. The Eight Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specific and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary, kept up to date.;
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. 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.
8. 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 data protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Sensitive Personal Data

Sensitive personal data means personal data consisting of information as to -

- The racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life
- The commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

4. Responsibilities

4.1 The school must:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them.
- Data held on obsolete equipment is to be disposed of by a trusted company, whose process must guarantee a signed and traceable procedure for the removal of data.

4.2 Every member of staff that holds personal information has to comply with the Act when managing that information.

4.3 The school is committed to maintaining the eight principles at all times. This means that the school will:

- Inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice and should be referenced on all forms/methods of data collection.
- Ensure the data subject has consented to the use of their personal data this should be opt in rather than opt out.
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act (see Appendix 1)
- Train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

4.4 This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

5. Complaints

Complaints should be made to the Chair of the board of Directors who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Enquiry/Information Line: 01625 545 700
Website: www.ico.gov.uk

6. Contacts

If you have any queries or concerns regarding, please contact
Headteacher Paul. Ackers (head@stjohnfisher.derby.sch.uk)
St John Fisher CVA
Alvaston Street
Alvaston
DE24 0PA
01332 572154

7. Policy Approval

Signature of Head teacher:

Signature of Chair of Directors

Date:

Date:

To be reviewed by March 2018

APPENDIX 1

Procedures for Requesting Information from the School

Requests for information under the Data Protection Act are called Subject Access Requests.

To access personal data, the request must be made in writing, which includes email, and be addressed to the Headteacher Mr P. Ackers. If the initial request does not clearly identify the information required, then further enquiries will be made.

A non-refundable fee of £10 will be charged in advance; the school will acknowledge receipt of the request as soon as possible after receipt of the payment of the fee. The response time for subject access requests, once officially received, is 40 calendar days. However, the 40 days will not commence until after receipt of fees or clarification of information sought. Any delay will be explained in writing to the person making the request.

Academies:

There is no equivalent legal right to access a pupil's educational record. The school will decide whether to grant such access, and it is likely to depend on the contractual relationship between the school and the parent.

1. Process

1.1 The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

1.2 Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into account 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 to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

1.3 The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

1.4 Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

1.5 Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

1.6 If there are concerns over the disclosure of information then additional advice should be sought.

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

1.7 Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

2. Feedback and Complaints

If you require further assistance or wish to make a complaint regarding information you have received or been refused, then initially this should be addressed to the Headteacher/Chair of Directors at St John Fisher CVA
Alvaston Street Alvaston Derby.

If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made, then this should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Data Protection Act 1998 and that deals with formal complaints. They can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Enquiry/Information Line: 01625 545 700
Website: www.informationcommissioner.gov.uk