Ofsted
Good
Provider

Data Protection Policy

Date approved: 21 January 2015
Signed by Chair of Governors: Mr Paul Rossi

Date approved: 21 January 2015
Signed by Headteacher: Mr Sean Hayes

Reviewed: January 2017
Next Review: January 2019

St John Fisher
Catholic High School

Data Protection Policy

General Statement

The Governing Body of St John Fisher Catholic High School has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.
The Headteacher and Governors intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988 and the Protection of Freedoms Act 2012. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the school's Data Protection Policy is available from the School Business Manager. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www. dataprotection.gov.uk).

Fair Obtaining and Processing

St John Fisher Catholic High School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

- **"processing"** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
- **"data subject"** means an individual who is the subject of personal data or the person to whom the information relates.
- **"personal data"** means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
- **"parent"** has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

Registered Purposes

The Data Protection Registration entries for St John Fisher Catholic High School are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from the School Business Manager who is the person nominated to deal with Data protection issues in the School. Registered purposes covering

the data held at the school are listed on the school's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity

The school undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.
Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. A printout of their data record will be provided to data subjects every twelve months so that its adequacy and relevance can be checked and agreed by the school centre and any amendments made.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Headteacher to ensure that obsolete data are properly erased.

Subject Access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil / student, the school's policy is that:

- Requests from pupils / students will be processed as any subject access request as outlined below and the copy will be given directly to the pupil / student, unless it is clear that the pupil / student does not understand the nature of the request.

- Requests from pupils / students who do not appear to understand the nature of the request will be referred to their parents or carers.

- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form, available from the School Office. Completed forms should be submitted to the School Business Manager. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.
Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

Authorised Disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.

- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.

- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.

- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **needs to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's / Centre's registered purposes. It is worth noting that comments on social media which disclose privileged personal data would fall into the category of "illegal disclosure".

Data and Computer Security

St John Fisher Catholic High School undertakes to ensure security of personal data in the following ways:

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Electronic Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly. Clearly, many documents in school contain sensitive and personal data. (For example, IEPs, SEN statements and annual reviews, exclusion letters) Great care must be taken when taking a copy of these documents off-site. Memory sticks containing personal and sensitive data should be encrypted and documents password-protected. Technical assistance with this is available from the IT Services Department in school.

Procedural Security

- In order to be given authorised access to the computer system, staff will have to undergo checks and will sign a confidentiality agreement.
- All staff are trained in their Data Protection obligations and their knowledge updated as necessary.
- Staff should not leave their computers logged on to personal data (for example SIMS) when they are not present in the room.
- Computer printouts as well as source documents are shredded before disposal.
- Students' school record files should not be taken off-site except under exceptional circumstances.
- Staff should avoid leaving documents containing personal and sensitive data in places easily seen by others; for example, left on desks at the end of the day.

Overall security policy for data is determined by the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of

this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Any queries or concerns about security of data in the school should in the first instance be referred to the School Business Manager

Further details on any aspect of this policy and its implementation can be obtained from: The School Business Manager at the school.

Approved by the Governors Finance and Premises Committee: 21 January 2015

Review Date: January 2019 Staff Member Responsible: Business Manager

Access to Personal Data Request (Data Protection Act 1998, Section7)

Enquirer Details:

Surname	
First Name(s)	
Address	
Postcode	
Telephone Number	

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?

YES / NO

If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?

YES / NO

If YES,

Name of Child	
Description of Concern / Area of Concern	
Description of Information or Topic(s) Requested	

Please despatch Reply to: ***(if different from enquirer's details as stated on this form)***

Surname	
First Name(s)	
Address	
Postcode	

Data Subject Declaration

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.
I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.
I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

……

Print Name of "Data Subject" (or Subject's Parent)

…….

Date ……..