

ST FRANCIS OF ASSISI CATHOLIC PRIMARY SCHOOL



DATA PROTECTION POLICY

Mission Statement

At St Francis of Assisi, we believe God is at the heart of our school. As a school community, we work together to provide a caring, stimulating and nurturing environment, where every child can discover their true potential and grow closer to Christ. As pupils and staff we encourage in each other a love of learning. This is a place where we can all belong and where diversity and difference is celebrated. We rejoice in each others' uniqueness and respect the dignity and beauty of each individual. Using our gifts and talents we will actively seek to make a real difference - by caring for one another and caring for our world.

Introduction

St Francis of Assisi Catholic Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. 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.

Schools 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 (<http://ico.org.uk/>). Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

The Governing Body of the 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 Head teacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1998.

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

Terms used in this document

- "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. ☒

Data Protection 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 specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
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.

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

Inform individuals why the information is being collected when it is collected

The 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. If details are given verbally, the person collecting will explain the issues before obtaining the information.

Inform individuals when their information is shared, and why and with whom it was shared

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 LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data. Confidentiality form to be completed by outside contractors.

Check the quality and the accuracy of the information it holds

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

Ensure that information is not retained for longer than is necessary

Data held about individuals will not be kept for longer than necessary for the purposes registered, the length of time will be determined by the Records Management Society of Great Britain Local Government Group Retention Guidelines for Schools (as amended).

Ensure that when obsolete information is destroyed that it is done so appropriately and securely

At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it. Automated systems can flag records for review, or delete information after a pre-determined period.

Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded

Schools are reminded that personal data and sensitive personal data as defined by the Data Protection Act should not be forwarded to personal email addresses as these do not have the required level of security.

Schools should ensure that all staff and governors use their school email address or Egress for secure transmission of mail. Schools should also ensure that this point is adequately addressed in the school's data protection/information governance policy. This will now be covered by internal audit as part of the audit process.

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.

Logical 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.

Procedural security

All staff will be trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

- 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.

Share information with others only when it is legally appropriate to do so

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 need to know the information in order to do their work.

The school will not disclose anything on pupils' records which would reasonably 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 registered purposes.

Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests

See appendix one

Ensure our staff are aware of and understand our policies and procedures

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Head teacher or nominated representative.

The next review of this document will be May 2018.

Contacts

If you have any enquires in relation to this policy, please contact the Head teacher who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, <http://ico.org.uk/> or telephone 01625 545745

Appendix one

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Head teacher, if the initial request does not clearly identify the information required, then further enquiries will be made.

2. 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.

3. 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.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records, schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Head teacher

5. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees or clarification of information sought

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

7. 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.

8. 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.

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

10. 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.

11. 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.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Signed Chair of Governors

Signed Head Teacher

Date: