St Edmund's Catholic School
A learning community
A faith community
A vibrant forward looking community

DATA PROTECTION STATUTORY POLICY

Reviewed by FGB 9th March 2016
Next review: March 2017

Kent County Council
Model Data Protection Policy Schools

St Edmund's Catholic School
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.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

2. The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

1. Data must 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 1998 Data Protection Act.
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 outside the EEA, 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.

3. Responsibilities

3.1 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.

3.2 The school has a legal responsibility to comply with the Act. The school, as a corporate body, is named as the Data Controller under the Act.

Date published	Policy review date	Agreed by:	Next Review
Dec 2013	9th March 2016	FGB	March 2017

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

3.3 The school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link : http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

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

3.5 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.
- 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)***
- train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures

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

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact

Michelle Hunt
Access to Information Co-ordinator
Children, Families & Education
Tel: 01622 696692
Email: michelle.hunt@kent.gov.uk

Appendix Responding to requests

Date published	Policy review date	Agreed by:	Next Review
Dec 2013	9th March 2016	FGB	March 2017

Taken from *The Guide to Data Protection, ICO*

The right of access to personal data.

What is an individual entitled to?

1 This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this and an individual who makes a written request and pays a fee is entitled to be:

• told whether any personal data is being processed;
• given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
• given a copy of the information comprising the data; and
• given details of the source of the data (where this is available).

3. In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request. (full details in section C2 of The Guide to Data Protection, ICO).

4. Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Neither are they entitled to information simply because they may be interested in it. So it is important to establish whether the information requested falls within the definition of personal data (see A32 – A316 of The Guide to Data Protection, ICO).

5. Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information.

6. Various exceptions to the right of subject access apply in certain circumstances or to certain types of personal data.

What is a valid subject request?

7 For a subject access request to be valid, it should be made in writing. You should also note the following points when considering validity:

• A request sent by email or fax is as valid as one sent in hard copy.

• You do not need to respond to a request made verbally but, depending on the circumstances, it might be reasonable to do so (as long as you are satisfied about the person's identity), and it is good practice to at least explain to the individual how to make a valid request, rather than ignoring them.

• a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, you may have to make a reasonable adjustment for them under the Equality Act 2010 (in Northern Ireland this falls under the Disability Discrimination Act 1995). This could include treating a verbal request for information as though it were a valid subject access request. You might also have to respond in a particular format which is accessible to the disabled person, such as Braille, large print, email or audio formats. If an individual thinks you have failed to make a reasonable adjustment, they may make a claim under the Equality Act (or Disability Discrimination Act 1995 in Northern Ireland).
Information about making a claim is available from the Equality and Human Rights Commission.

Date published	Policy review date	Agreed by:	Next Review
Dec 2013	9th March 2016	FGB	March 2017

•If a request does not mention the Act specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.

• A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure that you and your colleagues can recognise a subject access request and treat it appropriately.

Can I charge a fee for dealing with a subject access request?

13. Yes, an organisation receiving a subject access request may charge a fee for dealing with it. If you choose to do this, you need not comply with the request until you have received the fee. The maximum fee you can charge is £10.

What about requests for information about children?

26 Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong, for example, to a parent or guardian. So it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

27 Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should respond to the child rather than a parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

• the child's level of maturity and their ability to make decisions like this;

• the nature of the personal data;

• any court orders relating to parental access or responsibility that may apply;

• any duty of confidence owed to the child or young person;

• any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

• any detriment to the child or young person if individuals with parental responsibility cannot access this information;

• any views the child or young person has on whether their parents should have access to information about them.