St Chad's Catholic Primary School
Data Protection Policy

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

St Chad's Catholic Primary School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, St Chad's Catholic Primary School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Allow the subject of the information to see it on request.

St Chad's Catholic Primary School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The School has three/four Designated Data Controllers: They are the Headteacher, the School Administrator, the Senior Finance Officer and the School Business Manager.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be: The School Administrator.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.

- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g.about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Schools Data Protection Code of Practise.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Data Protection Code of Practise address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain

files. Any person who wishes to exercise this right should complete the Subject Access Request Form and submit it to the Designated Data Controller.

The School will make a charge of £10 on each occasion that access is requested, although the

School has discretion to waive this.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent

In many cases, the School can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the

Children Act 1989 and other enactments to ensure that staff are suitable for the job. The

School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users.

The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes.

The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy.

Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

Retention of Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Home Working/Off Site Working

Personal data processed on non school equipment is difficult to regulate and protect. In particular it is prone to non-authorised access such as by a relative or friend of the authorised member. It is the responsibility of the member of staff to ensure that all data pertaining to St Chad's is password protected.

All laptops, USB storage devices (e.g. memory sticks) and other mobile computing devices that access or store personal data should use data encryption software. This should apply to both school owned devices and any non-school owned devices which are used for school work.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

J Mooney

May 2016

Appendix 1

Data Protection Guidelines for Staff

Security

- The school building is fully alarmed whenever unoccupied.
- During school hours external gates are locked and access to the building is only through the security door at reception.
- Staff sign a Code of Conduct where they agree to keep information confidential.
- All personal data on paper is kept in the main school office, Head teacher's office or Deputy Head teacher's office in lockable filing cabinets.
- Personal data on the computer can be accessed only by authorised personnel using individual passwords. Passwords are changed regularly.
- The server is backed up externally.
- Laptops are not removed from the premises.

Procedures and protocols

- Personal data is rarely taken off site and only if absolutely necessary (e.g. for child protection conferences). The member of staff is responsible for the security of that information at all times.
- Information is transferred to new schools by either Royal Mail or internal mail in a sealed envelope.
- Child protection files are double enveloped and are sent by recorded delivery to a named person and marked private and confidential
- All information should be shredded which has:
  - children's full names
  - addresses
  - dates of birth
  - assessment data

Appendix 2

Subject Access Requests

Taken from Information Commissioners Office – Subject Access Code of Practice

A subject access request (SAR) is a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under section 7 of the Data Protection Act 1998 (DPA).

Requests for information about children

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 to anyone else, such

as 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. Before responding to a SAR 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 the parent. What matters is that the child is able to understand (in broad terms) what it means to make a SAR 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:

- where possible, 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; and
- any views the child or young person has on whether their parents should have access to information about them.

Information held about pupils by schools

A pupil, or someone acting on their behalf, may make a SAR in respect of personal data held about the pupil by a school. There are two distinct rights to information held about pupils by schools. They are:

- the pupil's right of subject access under the DPA; and
- the parent's right of access to their child's 'educational record'.Although this code is only concerned with the right of subject access, it is important to understand what is meant by a pupil's 'educational record'. This is because there is an overlap between the two rights mentioned above, and also because 'educational record' is relevant when ascertaining the fee you may charge for responding to a SAR. The statutory definition of 'educational record' includes most information about current and past pupils that is processed by or on behalf of a school. However, information kept by a teacher solely for their own use does not form part of the educational record. It is likely that most of the personal information a school holds about a particular pupil will form part of the pupil's educational record. However, it is possible that some of the information could fall outside the educational record; eg, information about the pupil provided by the parent of another child is not part of the educational record. Unlike the distinct right of access to the educational record, the right to make a SAR is the pupil's right. Parents are only entitled to access information about their child by making a SAR if the child is unable to act on their own behalf or has given their consent.

Examples of information which (depending on the circumstances) it might be appropriate to withhold include:

● information that might cause serious harm to the physical or mental health of the pupil or another individual;
● information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
● information contained in adoption and parental order records; and
● certain information given to a court in proceedings concerning the child.
If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days (if the school is in England, Wales or Northern Ireland). The maximum amount you may charge for dealing with the request depends on the number of pages of information to be supplied.

The following table shows the maximum fees.

Number of pages of information supplied	Maximum fee
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-69	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

If the SAR does not relate to any information that forms part of the educational record, then the usual 40-day time limit for responding applies. The maximum fee for dealing with the request is £10.

Appendix 3

Retention Schedule

Taken from the Records Management Toolkit for Schools produced by the Information and Records Management Society (May 2012)

A full list can be accessed on:

http://www.irms.org.uk/images/resources/infoguides/records_management_toolkit_for_schools_version_4_may_2012.pdf

File description	Retention Period
Child Protection files	DOB + 25 years
Allegation against a member of staff	Until persons retirement or 10 years from the date of allegation, whichever is the longer
Governor reports	Date of report + 6 years
Action plans	Date of action plan + 3 years
Policy documents	Expiry of policy
Complaints files	Date of resolution of complaint + 6 years
Minutes of SLT	Date of meeting + 5 years
School Development plans	Closure + 6 years
Admissions	Admission + 1 year
Admissions – if the appeal is unsuccessful	Resolution of case + 1 year
Proof of address as part of the admission process	Current year + 1 year
Admission registers	Date of last entry + 6 years
Attendance registers	Date of register + 3 years
Pupil files	Retain for the time the pupil remains at the school
SEN files, IEPs	DOB + 25 years
Correspondence relating to authorised absence	Date of absence + 2 years
Parental permission slips for school trips (where there has been no major incident)	Conclusion of the trip *(school recommendation is to retain for 1 month)*
Parental permission slips for school trips (where there has been a major incident)	DOB of the pupil involved + 25 years (permission slip for all pupils on the trip should be retained)
Class record books	Current year + 1 year
Pupils' work	Current year + 1 year
SATs records – papers and results	Current year + 6 years
Value added and contextual data	Current year + 6 years
Self-evaluation forms	Current year + 6 years

Staff personnel records	Termination + 7 years
Time sheets, sick pay	Current year + 6 years
Disciplinary proceedings oral warning	Date of warning + 6 months
Written warning – level 1	Date of warning + 6 months
Written warning – level 2	Date of warning + 12 months
Final warning	Date of warning + 18 months
Records relating to accident/injury at work	Date if incident + 12 years
Annual appraisal	Current year + 5 years
Maternity pay records	Current year + 3 years
Fire precautions log book	Current year + 6 years
Inventories of equipment and furniture	Current year + 6 years
Newsletters	Current year + 1 year
Visitors' book	Current year + 2 years
Annual accounts	Current year + 6 years
Budget reports and monitoring	Current year + 3 years
Invoices and receipts	Current year + 6 years
Annual budget	Current year + 6 years
Order books and requisitions	Current year + 6 years
Cheque books	Current year + 3 years
Paying in books	Current year + 6 years
Bank statements	Current year + 6 years
School journey books	Current year + 6 years
Free schools meals register	Current year + 6 years
Maintenance log books	Current year + 6 years
Dinner register	Current year + 3 years