St Erth Primary School

Data Protection Policy

St Erth School

Caring, Sharing, Preparing for Life

Date Written	Sept 2012
Reviewed On	November 2014
Last Review	
Next Review Date	November 2017
I confirm that this policy has been reviewed and adopted by the Governing Body of St Erth Primary School. Chair of Governors Date: Nov 2014	

Model Policy for Schools

Note:

This guidance is intended as an aide memoir as well as a pointer to the main principles of Schools Data Protection when drafting a policy. It is not and is not intended to be a complete statement of the law which is available from the extra reading sources noted at the end.

Introduction

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 Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.
In this document when we talk about a **data subject** we mean an individual who is the subject of the personal data or the person to whom the information relates. The term **processing** means obtaining, recording or holding the information or data.In all cases the term **personal data** will mean data which relates to a living individual who is identifiable

Section 1

1.1 Fair collection and processing

St Erth School takes its responsibility for collecting and using personal data very seriously and undertakes to do so both 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. Wherever possible, 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.

1.2 Registered purposes

The Data Protection Registration entries for the School are available for inspection, by appointment, at the school office.
Explanation of any codes and categories entered is available from the Senior Secretary 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.

1.2 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.
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. *(Details should be added on how and when records are checked for irrelevant data and who has the say on what must be deleted).*

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 Senior Secretary to ensure that obsolete data is properly erased. The school has its own Records Management Policy which will explain this in further detail.

How long records should be kept?

If you do not already have a records management policy or have a retention period for your records we would recommend using the Cornwall Council (education data) retention periods. The document can be found on schools messenger.

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 working 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.

On school websites or social media (for example if we use Facebook) we will ensure that we do not publish personal information (including images) without permission from the individual concerned. Access to websites and Facebook groups will be monitored by the School on a regular basis.

CCTV

Images of people are covered by the Data Protection Act, and so is information about people which is derived from images – for example, vehicle registration numbers. Where CCTV is used on school premises we will ensure that we tell people if it is in use.

1.3 Data and computer security

What is a 'data and computer security'?

A key responsibility for anybody that has responsibility to keep data is how securely it is kept. Breaches (losses) of personal data can mean huge monitory fines being levied against the school where loss of the data has been due to a security breach or as a result of physical loss of information. Breaches in data can also mean a loss of confidence in the school and reputational damage. You should seek guidance on system security if you want to ensure you are handling information safely.

You must take into account what the risk of losing or not appropriately handling data may be – for example a potential risk of harm, hacking of school systems, financial penalties – and ensure your systems "match" that level of security.

St Erth School undertakes to ensure security of personal data by the following general methods such as –

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 access to personal files. Information will be 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 including firewalls are installed on all computers containing personal data and are updated on a regular basis. Where needed, mobile devices, including phones, memory sticks and laptops are also encrypted. Only authorised users are allowed access to the computer files. Computer files are backed up (i.e. security copies are taken) regularly. Access to computer systems are password controlled and these passwords are changed regularly. Passwords are not shared with another person and are unique to the user.

1.5 Procedural security

What is a 'procedural security'?

This is about having processes in place to ensure that all your staff are no only aware of your school policy, system security or what to do if you receive a request for information but also that they have clear and defined procedures which they can follow. Training for all staff is recommended and the Information Commissioner has a free e-learning training package on their site which we recommend all school staff undertake: please visit www.bobs-business.co.uk.

All staff are 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 for data is determined by the Headteacher and is monitored and reviewed regularly, especially if a security breach becomes apparent.

Any queries or concerns about security of data in the school should in the first instance be referred to the Senior Secretary.

Individual members of staff can be personally liable in some circumstances in law under the terms of the Data Protection Acts. They may 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.

Section 2
Processing a Subject Access Request

Pupils have a right of access under the Data Protection Act 1998 to their own information. This is known as the right of subject access. When a child cannot act for themselves due to lack of capacity for example or the child gives explicit permission, parents will be able to access this information on their behalf.

As a parent, what sort of information can I access?
You have a right to access your child's educational record. This covers information that comes from a teacher or other employee of a local authority or school, the pupil or you as a parent, and is processed by or for the school's governing body or teacher, except for information the teacher has solely for their own use. So it will cover information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's governing body. It may also include information from the child and from you, as a parent. Information provided by the parent of another child would not form part of a child's educational record.

As a parent, how can I access to my child's educational record?
By making a request in writing to the Board of Governors.

How long should this take?
A request for an educational record must receive a response within 15 school days.
How much will it cost?
The school can charge what it costs to supply a copy of the information. Full guidance on charging can be obtained from the Information Commissioners Office and the school may refer to that guidance on a case by case basis to ensure it is charging in accordance with the Regulations.
As a parent, when can I request other information about my child?

You will be able to access all the information about your child if your child is unable to act on their own behalf or gives their permission. As a general guide, a child of 12 or older is expected to be mature enough to make this kind of request.

As a parent, are there circumstances where I could be denied access to my child's educational record?
There are certain circumstances where the school can withhold an educational record, for example, where the information might cause serious harm to the physical or mental health of the pupil or another individual.

As a pupil, what rights do I have to access my information?
You have (or someone acting on your behalf has) the right to a copy of your own information. This is known as the right of subject access. However, schools may withhold information in certain circumstances, such as where serious harm may be caused to your physical or mental health or another individual, or where the request is for an exam script or for exam marks before they are officially announced.

What if the information you want involves information about another person?
Information about another person may not always be available to you. Unless the other person gives their permission, or it is reasonable in the circumstances to provide the information without permission, the school will be entitled to withhold this information.

Recommended template form for schools to use

Access to personal data request

Surname

Forenames

Enquirer's Address

Enquirer's Postcode

Telephone Number

Are you the person who is the subject of the records you are enquiring about	YES / NO
If NO, Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?	If YES, Name of child or children about whose personal data records you are enquiring …… …….. …… …….. …… ……..

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Please send reply to

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) ……

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

(PRINTED)…….
Dated …….

Prepared by: Samantha Hocking

Samantha Hocking, Data Protection and Freedom of Information Officer, Children Schools & Families. County Hall Truro

This policy was adopted by the Governing Body of St Erth School in October 2014 for review in October 2016.

If you would like this information in another format please contact:

Cornwall Council County Hall Treyew Road Truro TR1 3AY

Telephone: **0300 1234 100**

Email: **enquiries@cornwall.gov.uk**

www.cornwall.gov.uk