Data Protection Policy

Introduction

St John's Primary School recognises and accepts its responsibility as set out in the Data Protection Act 1998. The School, as a Data Controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information.

This policy statement applies to all School governors and employees, and individuals about whom the School processes personal information, as well as other partners and companies with which the School undertakes it business.

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. 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

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

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.

The School needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, pupils, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 1998.

We regard the lawful and correct treatment of personal information by the School as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The School will treat personal information lawfully, correctly and in compliance with the 1998 Act.

February 2016

Fair Obtaining and Processing

St John's 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.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

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.

Aims and Objectives

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
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- 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
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests

February 2016

- Ensure our staff are aware of and understand our policies and procedures
- Ensure there is someone with specific responsibility for data protection in the organisation. (Currently, the nominated person is the Business Manager);

Data and Computer Security

St John's undertakes to ensure security of personal data by the following general methods:

- **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. Printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear visitor 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 and centrally.

- **Procedural Security**

In order to be given authorised access to the computer, 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. 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.

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

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.

Monitoring & Review

A copy of this policy statement will be issued to all employees. It will be reviewed periodically, added to, or modified from time to time and may be supplemented in appropriate

cases by further statements and procedures relating to the work of the particular groups of workers.

To be reviewed: May 2018

Appendix 1

St John's Primary school - Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.
1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Business Manager**.** 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 Headteacher 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, dependant upon the following:
   - Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.

February 2016

- 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 Headteacher.

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.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

February 2016

Contacts
If you have any queries or concerns regarding these procedures then please contact Tracey Caffrey**,** Headteacher.
Appendix 2

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname……
Enquirer's .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 (i.e. the "Data Subject")?

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 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)

Additional information.

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

Name:

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) ……

Name of "Data Subject" (or Subject's Parent) (PRINTED)…….

February 2016

Dated …….

February 2016