Data Protection Policy

Updated: October 2016
Review Date: Autumn 2018

1. POLICY STATEMENT

1.1

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our pupils, their parents and our staff and we recognise that the correct and lawful treatment of this data will maintain confidence in the school. St Christopher Primary School is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. The school is a data controller and, as such, is registered with the Information Commissioners Office and complies with the principles of the Data protection Act 1998.

1.2

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

This policy statement applies to the following:

i) Employees, including temporary, contractual and agency;
ii) Governors;
iii) People, partner agencies, organisations, volunteers, students or any other authorised person contracted to work or process personal information on behalf of the School.

2. ABOUT THIS POLICY

2.1

St Christopher Primary School needs to keep certain information about our employees, pupils and other users to allow us to comply with statutory duties and for other matters such as, to monitor performance, achievement, and health and safety.

2.2

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3

This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4

This policy has been approved by the Governors. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5

The School has identified its Designated Data Officer as the Headteacher. They will have overall responsibility for Data Protection within the School.

2.6

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 Headteacher, in the first instance.

3. DEFINITION OF DATA PROTECTION TERMS

3.1

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2

Data subjects, for the purpose of this policy, include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5

Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition.

3.7

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data for or on behalf of us must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully and shall not be processed unless specific conditions are met.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate and kept up to date where necessary.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Appropriate technical and organisational controls will be applied to protect personal data from unauthorised and unlawful processing and against accidental loss, destruction or damage.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. NOTIFICATION

We will maintain our entry on the Information Commissioner's public register of data controllers.

6. RISKS

We recognise that there are risks associated with the processing of personal data. This policy statement aims to mitigate risks such as:

i) Loss of confidence in the School's ability to safeguard personal data;
ii) Loss of reputation and damage to the School's corporate image;
iii) Ineffective management of information security incidents;
iv) Inadequate controls for managing access to, retention and disposal personal data;
v) Legal, regulatory or financial penalties.

7. DATA SECURITY

7.1

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

7.2

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

7.3

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore always be stored securely and password protected if electronic. If a data is kept on a removable storage device, that device will be password protected and/or kept in a secure location.

7.4

We are responsible for information that is held not only on equipment owned by us, but personal equipment that we know is being used by our employees or other authorised people/organisations. Consequently the use of privately owned equipment or removable media devices for processing personal data on our behalf is prohibited unless a documented risk assessment has been undertaken and appropriate controls are implemented to safe guard personal data from deliberate, unintentional or unauthorised access, modification, destruction or disclosure.

8. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

8.1

We may share personal data we hold with Coventry City Council in their role as the Local Education Authority and in line with legal obligations.

8.2

We may also disclose personal data in compliance with any Child Protection legislation or legal obligation.

8.3

If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or to protect our rights, property, or safety of our employees, pupils, or others.

8.4

Contractual and/or data processing agreements will be established and maintained when an external person or organisation is processing personal data on our behalf.

9. DEALING WITH SUBJECT ACCESS REQUESTS

9.1

Any data subjects whose details are held or processed by us have a general right to receive a copy of their own information under the Data Protection Act 1998.

9.2

There are a number of exemptions to this right under the Data Protection Act, such as data held for child protection or crime detection/prevention purposes and in these circumstances, we are able withhold any relevant information. We will implement and maintain processes and procedures to support the correct and consistent application of exemptions.

9.3

We will respond in writing to requests for access to pupil records within 15 school days for requests made in line with the Education (Pupil Information) (England) Regulations 2005 and for all other types of Data within

the 40 days allowed by the Data Protection Act.

9.4

A subject access request should be submitted in writing to ensure that the school has the required information to be able to conduct a data search and fulfil the request. The request must also supply the relevant information to enable us to accurately identify the requestor.

In some cases, further information may be required from the requester which may delay the start of the 40-day maximum period.

9.5

We will only deal with a request for subject access in respect of a pupil if:

a) Requests from parents / legal guardians in respect of their own child will, provided that the child does not understand the nature of the subject access requests, be processed as requests made on behalf of the data subject (child)

b) Requests from pupils who do not understand the nature of the request will be referred to the child's parents/guardians.

c) Requests from pupils who demonstrate an understanding of the nature of their request will be processed as any subject access request.

d) Any decision regarding whether or not a child has the necessary level of understanding will be made by our Designated Data Officer.

9.6

Where information is not available from the school but is processed by the Local Authority (such as admissions and transfers) the requests will be directed to the appropriate officer.

9.7

The School will not normally charge for processing requests, but this will be reviewed in the light of the numbers and types of requests received. If a decision is made to charge, the fee will be based on the current guidance supplied by the Information Commissioners Office.

Where information is requested under the Education (Pupil Information) (England) Regulations 2005 the fee payable for copies of pupil records will be as prescribed by the Governing Body of the School.

9.8

Repeat requests will be fulfilled unless deemed unreasonable, such as a second request received so soon after the first that it would be impossible for the details to have changed.

9.9

We will maintain a register of requests for access to personal information.

10. RETENTION OF DATA

We have a duty to retain some staff and pupil and other personal data for a period of time following their departure from the School, in compliance with relevant legal duties.

11. INFORMATION SECURITY INCIDENTS

11.1

Data users must immediately (or as soon as practicable) report any actual or suspected breaches of information to the Headteacher.

11.2

Reported incidents will be investigated and reported on;

11.3

Data users must immediately (or as soon as practical) report IT equipment that has been lost or stolen to the School Business Manager.

TRAINING AND AWARENESS

We will provide appropriate training and awareness for data users.

13. MONITORING

Compliance with this policy and supporting framework will be undertaken by a combination of methods, including but not limited to: ad hoc quality checks by the Headteacher, internal and/or external audits, and day to day operational activities.

14. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time and in any event on a periodic basis. Reviews will take into account changes in legislative practices and guidance from the Information Commissioner's Office.