School Data Protection Policy

Christopher Reeves VA Primary School.
Hinwick Road, Podington

January 2018

Review date: Spring Term 2019

Committee responsible: Personnel

Christopher Reeves VA Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

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 Privacy 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 from 25th May 2018, The General Data Protection Regulations 2018. 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.

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

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 / General Data Protection Regulations 2018;

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.

General Statement

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
- Ensure our staff are aware of and understand our policies and procedures

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Signed ……. Headteacher

……..Chair of Governors

Date …….. Review Date ……..

Contacts

If you have any enquires in relation to this policy, please contact Mrs Juliet Fraser (Headteacher) who will also act as the contact point for any Subject Access Requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk

Appendix 1 - Subject Access Requests

Procedures for responding to subject access requests made under the Data Protection Act 1998 / General Data Protection Regulations 2018

Rights of access to information

Under the GDPR 2018, any individual, or Data Subject, has the right to access their personal data held by the school. One of the ways they can do this is through a **Subject Access Request**, which can be a request to see part or all of the data held. A parent / guardian will act on behalf of children under the age of 12.

This may lead to a request to change details if they are inaccurate, which is part of the Data Subject's **Right to Rectify.**

The Data Subject may also exercise their **Right to Erasure** (if unnecessary data is held) and their **Right to Restrict Processing**, however, there will be certain situations where the school cannot grant this because of its legal statutory responsibilities. This will be clearly explained to the Data Subject making the request.

Actioning a Subject Access Request

1. Requests for information may be made verbally, electronically or in writing, and be addressed to Mrs Juliet Fraser (Headteacher). If the initial request does not clearly identify the information required, then further enquiries will be made.

2. Every request will be logged on a central record, noting the requestor, specific data requested, the date the request was made and the date by which a response will be received.

3. 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, if the child is the Data Subject. Evidence of identity can be established by production of:
    - passport
    - driving licence
    - utility bills with the current address
    - Birth / Marriage certificate

4. The response time for Subject Access Requests, once officially received, is no more than **one calendar month**, irrespective of school holidays. The school aims to respond much more quickly than this, however, parents will need to be aware that school holiday periods will make this more difficult. The speed of the response will also depend on the amount of data requested. Finally, if the request is deemed complex, the Data Subject will be informed within one calendar month, and the school will have a further **two calendar months** to produce the data.

5. The responsibility to keep children safe (safeguarding) may prevent disclosure of some information. If there are concerns over the disclosure of information then additional advice will be sought.

6. Information provided as a result of a Subject Access Request will be clear and understandable, so that any codes or technical terms may need to be clarified and explained. 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. If the data is being sent by post, registered/recorded mail must be used.

Appendix 2 - Data Breach Procedures

A Personal Data Breach is when a breach of security leads to the accidental or unlawful loss, destruction, alteration or disclosure of personal data.

Preventing Personal Data Breach

The school takes significant measures to ensure that the data held is done so securely, and has processes in place to minimise the risk of a breach.

These risks and measures include:

- loss / theft of data (e.g. individually secured cabinets and cupboards, locking of controlled offices, locking / alarming of school buildings.)
- loss / theft of equipment on which data is stored (e.g. encrypted devices, password protection of documents and equipment, secure email systems to the Local Authority)
- inappropriate access to controlled areas in the school (e.g. control of visitor / tradesmen access)
- human error (e.g.email retrieval)

Data Breach Recording

The school will record all data breaches, no matter how small, in order to inform and improve our risk management of a serious data breach. Data breaches may be deliberate or accidental.

The definition of a serious data breach is that the loss, destruction, alteration or unauthorised disclosure interferes with the rights and freedoms of the data subject(s). In the unfortunate event of a serious data breach, we will notify the Information Commissioner's Office (ICO) www.ico.gov.uk and are required to do so **within 72 hours** of the breach.

If the serious data breach is likely to result in a high risk of adversely affecting the individuals' rights and freedoms, we will also inform the individual data subject(s) without delay.

Responding to a Data Breach

In addition to our responsibility to record the breach, inform the ICO and where appropriate the data subject(s) affected, the school will investigate the cause of the data breach and take corrective steps, altering our risk management accordingly.

The circumstances may require the school to notify third parties, such as the police and our insurers.

Appendix 3 - Data Retention Schedule

The education sector is currently considering a data retention strategy, and the school will adopt the recommendations once these are agreed. In the meantime, we are working to the following guidelines:

Data	**Retention Period**
Primary School Record (attainment & progress)	5 years after pupil leaves
Pupil data	1 year after pupil
Parental Details	1 month after pupil leaves
Safeguarding Records	Until the subject is 25 years old
Health / Accident records	Until the subject is 25 years old