

Simonside Primary School



Data Protection Policy

Sept 2016

To be reviewed: July 2017

SIMONSIDE 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

Simonside Primary School needs to keep certain information about its employees, parents and pupils and other users to allow it to monitor performance, achievements, and ensure safeguarding.

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, Simonside 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.

Simonside 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.

Responsibilities of staff and parents

All staff and parents are responsible for:

- Checking that any information that they provide to the School about themselves or their child is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, contact numbers etc. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

The Data Controller, Senior Information Risk Owner and Information Asset Owner

Data Controller

The school as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation.

The Senior Information Risk owner

The SIRO is a member of the Senior Leadership Team and has the following responsibilities:

- They own the Data Protection Policy and Information Risk Assessment which includes:
 - The assets involved
 - Legal requirements (such as Data Protection Act 1998).
 - The practicalities of running the organisation day to day.
 - The impact of incidents on the reputation of the school in the community.
- They appoint the Information Asset Owners (IAOs).
- They act as an advocate for information risk management.

Information Asset Owners

The school has identified the following information assets:

- Management Information System Data (SIMs)
- Financial Data
- Organisational & Operational Data
- Correspondence
- Assessment Data
- Pupil Work and Progress Evidence
- Any other data.

An Information Asset Owner is identified for each asset. The role of the IAO is to understand and to communicate to other staff:

- What information is held, and for what purpose.
- How information will be amended or added to over time.
- Who has access to the data and why.
- How information is retained and disposed of.

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.

Data Storage

- 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 a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Processing, storing, archiving and deleting personal data: guidance

- Personal data and school records about pupils are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when pupils change schools.
- School and examination records on a child should be kept until their 25th birthday. Data on staff is sensitive information and confidential to the individual, and is shared, where appropriate, at the discretion of the Head Teacher and with the knowledge, and if possible the agreement of the staff member concerned.
- Employment records form part of a staff member's permanent record.
- Interview records, CV's and application forms for unsuccessful applicants are kept for 6 months securely in school.
- All formal complaints made to the Head Teacher or School Governors will be kept in for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.

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.

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 or volunteers 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, parents (and pupils where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment or to volunteer 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, parent and pupil 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.

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.

September 2016