Simonside Primary School
Data Protection Policy

1. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- how staff, parents and pupils can access personal data.

1.1. It is a statutory requirement for all schools to have a Data Protection Policy:

(http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

1.2. Data Protection Principles

The Data Protection Act 1998 establishes eight 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.

2. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. The DPA defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach" which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

2.1. Personal data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

2.2. Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and biometric data. It requires a greater degree of protection and in a school would include:

- Staff Trade Union details
- Information on the racial or ethnic origin of a pupil or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff
- Some information regarding safeguarding will also fall into this category.

2.3. Other types of Data not covered by the act

This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA - this may fall under other 'access to information' procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provides additional information on their website. See http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

3. Responsibilities

The Head Teacher and Governing Body are responsible for Data Protection, they will appoint a Data Protection Officer to manage data.

3.1. Risk Management – Roles: *Data Protection Officer*

The school has a nominated member of staff responsible for the management of data protection.

According to the ICO the minimum role will include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

3.2. Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.

- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

4. Legal Requirements

4.1. Registration

The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration:
http://ico.org.uk/for_organisations/data_protection/registration

4.2. Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils and staff of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through a letter.
More information about the suggested wording of privacy notices can be found on the DfE website:
http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

5. Transporting, Storing and Disposing of personal Data

The policy and processes of the school will comply with the guidance issued by the Information Commissioner's Office.

Here is a summary of the ICO recommendations under each section:

- Notification – make sure you notify us accurately of the purposes for your processing of personal data.
- Personal data – recognise the need to handle personal information in line with the data protection principles.
- Fair processing – let pupils and staff know what you do with the personal information you record about them. Make sure you restrict access to personal information to those who need it.
- Security – keep confidential information secure when storing it, using it and sharing it with others.
- Disposal – when disposing of records and equipment, make sure personal information cannot be retrieved from them.
- Policies – have clear, practical policies and procedures on information governance for staff and governors to follow, and monitor their operation.
- Subject access requests – recognise, log and monitor subject access requests.
- Data sharing – be sure you are allowed to share information with others and make sure it is kept secure when shared.
- Websites – control access to any restricted area. Make sure you are allowed to publish any personal information (including images) on your website.
- CCTV – inform people what it is used for and review retention periods.
- Photographs – if your school takes photos for publication, mention your intentions in your fair processing/privacy notice.
- Processing by others – recognise when others are processing personal information for you and make sure they do it securely.

- Training – train staff and governors in the basics of information governance; recognise where the law and good practice need to be considered; and know where to turn for further advice.
- Freedom of information – after consultation, notify staff what personal information you would provide about them when answering FOI requests.

5.1. Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

5.1.1. Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). This can be done by pressing Ctrl, Alt, Del and then clicking on Lock this computer.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (ie owned by the users) must not be used for the storage of personal data.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

5.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete
- Only encrypted removable storage purchased by the school is allowed to be used on school computers.

5.1.3. Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

5.1.4. Images

- Images of pupils will only be processed and transported by use of.encrypted devices.
- Images will be protected and stored in a secure area.
- (**This is in the Photographs folder on the teachers shared drive on the Server**).

5.1.5. Cloud Based Storage

- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example *Onedrive*) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data. See advice from the DfE below:-

https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

5.2. Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party as well as data processing agreements.
http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

5.3. Retention of Data

- The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
- Personal data that is no longer required will be destroyed and this process will be recorded.

5.4. Systems to protect data

5.4.1. Paper Based Systems

- All paper based personal data will be protected by appropriate controls, for example:
- Paper based safeguarding chronologies will be in a locked cupboard when not in use
- Class Lists used for the purpose of marking may be stored in a teacher's bag.

- Paper based personal information sent to parents (will be checked by Office staff and class teacher before the envelope is sealed).

5.4.2. School Websites

- Uploads to the school website will be checked prior to publication, for instance:
- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded.

5.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- Where technically possible all e-mail containing sensitive information will be encrypted by *(*by attaching the sensitive information as a word document and encrypting the document / compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password).

6. Data Sharing

The school is required by law to share information with the LA and DfE. Further details are available at:
https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

Schools should ensure that, where data that is shared, it is transmitted securely for instance by secure e-mail.

7. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach the data protection officer will inform the Head Teacher and Chair of Governors.
- The school will follow the procedures set out in Appendix 7~ summarised below.

Record the following in a log if known:

a) Date of incident
b) Date you were made aware of the potential breach
c) Location of incident
d) Nature of incident, that is, is it a loss, theft, disposal, unauthorised disclosure?
e) Nature of data involved, list all data elements. For example, whether it is names, files, dates of birth, or reference numbers
f) What security protection was on the data? Is it protected by a password, encryption, or something else?
g) Is there a back up of the data, if so where?
h) Number of people potentially affected, an estimate should be provided if no precise figure can be given.

i) Details of any steps taken to retrieve data or to contain the breach if it involved unauthorised access or potentially compromised security.

The log can then be analysed to ensure that any lessons learnt from breaches can be implemented.

8. Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years or when legislation changes.

Date: 8.10.18 Review: 8.10.20

Adopted by the Governing Body on 8.10.18

The Data Protection Officer is Chapman Data and Information Services Ltd., 29 Hardie Drive, West Boldon, NE36 0JH.