Wolsingham Primary School

Data Protection Policy

Reviewed and accepted:
Chair of Governing Body: P. Eastwood
Headteacher: S. Kitching
Date: May 2018
Date for Review: May 2020

Aims & Objectives

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with current UK and EU legislation.

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 deleted/destroyed
- How staff, parents and pupils can access personal data
- This policy applies to all data, regardless of whether it is in paper or electronic format.

Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
EEC	European Economic Community

Legislation and guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

It also takes into account the expected provisions of the **General Data Protection Regulation**, which is new legislation which come into force in 2018.

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In Addition article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

Lawful Basis for processing data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that schools collect and process is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that a school is likely to rely on.

There are other bases that may be available, such as a specific legal obligation applying to the data controller that makes the processing necessary. Your legal advisor will be able to identify individual statutes if required.

Age

Children under the age of 13 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians do this on their behalf. Over the age of 13 this responsibility is transferred to the child and parents will not have responsibility for their child's data. (This is subject to the Data Protection Bill becoming law. The 'default' age under the GDPR is 16.)

Consent

If there is a lawful basis for collecting data then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

Rights

The GDPR creates some new rights for individuals and strengthens some existing ones. It provides for the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Different rights attach to different lawful bases of processing:

	Right to erasure	**Right to portability**	**Right to object**
Vital Interests	✓	X	X
Legal Obligation	X	X	X
Public Task	X	X	✓
Legitimate Interests	✓	X	✓
Contract	✓	✓	X
Consent	✓	✓	X but right to withdraw consent

The right to erasure

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Your legal advisor will be able to support with information about which data can continue to be legally held if a data subject asks to be 'forgotten'. Schools' data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that where a school relies on either a ‘legal obligation’ or a ‘public task’ basis for processing (see above) there is no right to erasure – however this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school’s data retention guidelines.

Data Types

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 and members of the Governing Body 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.

Special Category Data

“Special Category Data” are data revealing a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person’s health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

This includes:

- 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 (SEND)
- (Some information regarding safeguarding will also fall into this category.) staffing e.g. Staff Trade Union details

Roles and responsibilities

The head teacher and governing body has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998.

The Data Controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is the data controller.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

Data Protection Officer

The school must have a nominated member of staff responsible for the management of data protection. Here at Wolsingham Primary School this is Mrs S. Kitching (Headteacher). It is the responsibility of the DPO to:

- inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- 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
- be the first point of contact for supervisory authorities and for individuals whose data is processed.

Staff and Governors Responsibilities

Day-to-day responsibilities for ensuring the school is compliant with data protection regulations rest with the Headteacher or the Deputy Headteacher in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

- 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.

Privacy/fair processing notice

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals

where we are processing their personal data. Our privacy notices **must** inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed.

All privacy notices will be distributed to staff/parents/carers through both digital and written channels.

Subject access requests

Under the Data Protection Act 1998, pupils and staff have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter or email. Requests should include:

- The data subjects name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- Information relating to other data subjects, including names of other children or members of staff within the request. School have a legal obligation to redact this information from any documents within the data subject request.

Subject access requests for all or part of a pupil's educational record or staff will be provided within 40 days free of charge. However if the request is manifested unfounded or excessive, particularly if the request is repetitive then school have the right to charge a fee to comply with requests or to provide additional copies of information. Fees are based on the administrative costs of providing the information and can be provided upon request.

Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 40 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 13 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil. Parental responsibility ceases to apply once a child reaches 18. Students aged 18 and over may therefore prevent their parents from accessing their educational information.

If parents ask for copies of information, they will be required to pay the cost of making the copies.

Transportation, Storage and deletion of data

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) and set to auto lock if not used for ten minutes.
- 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 (where allowed). Private equipment 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.

Portable Devices

- School has a strict policy on the use of portable devices including laptops, full details on the use of portable devices can be found in the school acceptable use policies.
- Personal data must not be accessed on any portable device other than school issued
- Where necessary the data must be encrypted and password protected
- Any school issued portable device must be password protected and encrypted
- Any portable device issued by school can be remotely locked and if required, securely erased

School Requirements

- All users will use strong passwords which must be changed regularly. User passwords must never be shared.
- Images of pupils will not be processed off site, the only exception to this is press photography and the school photographer in which case written permission for this will be obtained in advanced.
- All images will be protected and stored in a secure area on the school network.
- School has clear policy and procedures for the use of “Cloud Based Storage Systems” 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 the cloud based data services providers to protect the data.
- 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.

Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example:

- Paper based documents containing any data will be in a locked cupboard or drawer
- Child protection and 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 locked drawer.
- Paper based personal information sent to parents will be checked by two members of staff, before the envelope is sealed.

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.

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 attaching the sensitive information as a word document and encrypting the document or using a password on files and folders. The recipient will then need to contact the school for access to a one-off password)
- The use of Egress (Secure e-mail system) allows for secure communication.

Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

Training

Our staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018.

We will review working practices when this new legislation takes effect and provide training to members of staff and governors where appropriate.

Monitoring arrangements

The Headteacher is responsible for monitoring and reviewing this policy.

The Headteacher and chair of governors checks that the school complies with this policy by, among other things, reviewing school records on a termly basis or sooner if required.

This document will be reviewed when the General Data Protection Regulation comes into force, and then every two years.

At every review, the policy will be shared with the governing body.

Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.