DATA PROTECTION POLICY

Committee Responsible:	Finance and Resources
Person Responsible:	Headteacher
Date Approved by FGB:	April 2018
Date for Review:	April 2019

Signed……..

Date……..

Contents

1. Aims

This Policy will ensure:

- The School processes personal data fairly and lawfully and in compliance with the Data Protection Principles.
- All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities under this policy.
- That the data protection rights of those involved with the School community are safeguarded.
- Confidence in the School's ability to process data fairly and securely.

2. 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 (ICO) and model privacy notices published by the Department for Education.

It also takes into account the provisions of the General Data Protection Regulations (GDPR) and 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 and section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

3. 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

4. The Data Controller

The School processes personal information relating to pupils, staff, volunteers (including governors) and visitors, and, therefore, is registered as a data controller with the Information Commissioner's Office and renews this registration annually. Details of the School's purpose for holding and processing

data can be viewed on the data protection register: https://ico.org.uk/esdwebpages/search

The Schools registration number is Z7189235. This registration is renewed annually and up dated as and when necessary.

5. Data Protection Principles

Article 5 of the GDPR sets out six data protection principles which must be followed at all times:

- personal data shall be processed fairly, lawfully and in a transparent manner;
- personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- personal data shall be adequate, relevant and limited to what is necessary for the purpose(s) for which it is being processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
- personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The School has processes for dealing with the exercise of the following rights by governors, staff, pupils, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed, how it is stored and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including profiling.

6. Roles and Responsibilities

The governing board has overall responsibility for ensuring that the school complies with its Data Protection obligations.

Day-to-day responsibilities rest with the Headteacher, or the School Business Manager 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.

Complaints about data processing will be dealt with in accordance with the Schools Complaints Policy.

7. Privacy/Fair Processing Notice

Pupils and Parents

The School holds personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. It may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Attendance information
- Details of any medical conditions

The School will only retain the data it collects for as long as is necessary to satisfy the purpose for which it has been collected.

The School will not share information about pupils with anyone without consent unless the law and the School policies allow it to do so. Individuals who wish to receive a copy of the information that is held about them/their child should refer to sections 8 and 9 of this policy.

The School is required, by law, to pass certain information about pupils to specified external bodies, such as the local authority and the Department for Education, so that they are able to meet their statutory obligations.

Staff

The School processes data relating to those it employs to work at, or otherwise engage to work at, the school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform the recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

The School will only retain the data it collects for as long as is necessary to satisfy the purpose for which it has been collected.

The School will not share information about staff with third parties without consent unless the law allows it to.

The School is required, by law, to pass certain information about staff to specified external bodies, such as the local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the School Business Manager.

8. Subject Access Requests

Pupils 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, email or fax. Requests should include:

- The pupil's 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

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days. The School may charge for providing the information and if this is the case it will be in accordance with Local Authority Regulations.

If a subject access request does not relate to the educational record, the School will respond within one calendar month. Where requests are complex or numerous the period for compliance may be extended by a further two months. In this case the individual will be informed within one month of the receipt of the request with an explanation as to why the extension is necessary.

9. Parental Requests to See the Educational Record

Parents have the right of access to their child's educational record, free of charge, within 15 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 generally regards children aged 12 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 this school may be granted without the express permission of the pupil.

10. Data Security and Data Security Breach Management

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with the Schools Acceptable IT Use Policy.

The School has a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with the GDPR.

All staff will be aware of and follow the data breach security management process.

The School will ensure the following:

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use;
- Papers containing confidential personal information are not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access;
- Where personal information needs to be taken off site (in paper or electronic form), staff sign it in and out from the school office;
- Passwords with at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.

All staff will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix A

11. Disposal of Records

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

For example, the School will shred or incinerate paper-based records, and override electronic files.

The School may also use an outside company to safely dispose of electronic records.

12. Training

The 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.

Appendix

What staff should do:

DO get the permission of your manager to take any confidential information home.

DO transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.

DO use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.

DO ensure that any information on USB memory sticks is securely deleted off the device or saved on a School shared drive.

DO ensure that all paper-based information that is taken off the premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.

DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.

DO ensure that paper-based information and laptops are kept safe and close to hand when taken out of the premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).

DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.

DO return the paper-based information to the School as soon as possible and file or dispose of it securely.

DO report any loss of paper-based information or portable computer devices to your line manager immediately.

DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.

DO ensure that when posting/emailing information that only the specific content required by the recipient is sent and password protection is used where appropriate.

DO use pseudonyms and anonymise personal data where possible.

DO ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.

What staff must NOT do:

DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.

DO NOT unnecessarily copy other parties into e-mail correspondence.

DO NOT e-mail documents to your own personal computer.

DO NOT store work related documents on your home computer.

DO NOT leave personal information unclaimed on any printer or fax machine.

DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.

DO NOT leave documentation in vehicles overnight.

DO NOT discuss case level issues at social events or in public places.

DO NOT put confidential documents in non-confidential recycling bins.

DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.

DO NOT use unencrypted memory sticks or unencrypted laptops