DATA PROTECTION POLICY AND PRIVACY NOTICE

April 2018

Created by	Senior Management and Governors
Date	April 2018
Reviewed by	Verity McAuley, SBM / Wendy Perry, HR Manager
Date	April 2018
Ratified by Governors	10.06.2020
Next review date	April 2021

1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998.

This policy applies to all data, regardless of whether it is in paper or electronic format.

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 and model privacy notices published by the Department for Education.

It also takes into account the expected provisions of the General Data Protection Regulations, which is new legislation due to come into force in May 2018.

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.

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 who determines the purposes for and the manner in which any personal data is held, or to be processed. In a school setting this will be a school leader.
Data processor	A person who processes data on behalf of the data controller (e.g. a school's payroll provider). A school may also process its data, in which case the school is also the data processor (e.g. the school's administrators)
Data Protection Officer (DPO)	A person who is responsible for the overall compliance with GDPR. It should be someone with sufficient expertise and independence. In a school, the DPO is likely to be a senior leader or governor.

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the School Business Manager.

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

5. Data protection principle

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

6. Roles and responsibilities

The Governing Board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998 and any subsequent changes of legislation.

Day-to-day responsibilities rest with the Executive Headteacher, or the Head of Campuses in the Executive Headteacher's absence. The Executive 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.

7. Privacy/fair processing notice

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We 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
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

Once our pupils reach the age of 13, we are legally required to pass on certain information to Bournemouth Youth Support Services which has responsibilities in relation to the education or training of 13-19 year-olds. Parents, or pupils if aged 16 or over, can request that only their name, address and date of birth be passed to Bournemouth Youth Support Services by informing the School Data Administration Officer.

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

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our 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 our 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

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected, and in any case in line with our Retention and Destruction of Records procedures.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our 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 Linwood HR Manager and make a subject access request application which will be provided to them within 30 days at no cost, as described in section 8.

8. Subject access requests

Under the Data Protection Act 1998, 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 30 days..

Unfounded or excessive requests may be charged for or even refused.

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.

Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

10. Storage of records

- 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 should 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 must sign it in and out from the school office
- Passwords that are 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. No unencrypted device should be used by any member of staff, in line with the ICT Acceptable Use Policy Agreement.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

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, 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.

12. Training

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

13. Data Protection Privacy Impact Assessments (PIAs)

PIAs are tools that can help schools to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. A PIA is only required in high – risk situations, for

example where new technology is being deployed. The ICO can be contacted to confirm whether or not data amounts to a high risk situation.

14. Data Breaches

Certain personal data breaches will have to be reported to the Information Commissioning Office (ICO). These include breaches where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach. Where a breach could result in a high risk to the rights and freedoms of individuals, ICO should be notified. Failure to report a relevant breach within 72 hours of the actual breach could result in a fine on top of a fine for the breach itself.

15. 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 continue to monitor any changes to legislation and will review working practices as required. We will provide training to members of staff and governors where appropriate.

16. Monitoring arrangements

The Executive Headteacher and Governing Board are responsible for monitoring and reviewing this policy.

The Data Protection Officer checks that the school complies with this policy by, among other things, reviewing school records.

This document has been reviewed in light of the General Data Protection Regulation fully coming into force in May 2018. It will then be reviewed in April 2019 and thereafter.

At every review, the policy will be shared with the Governing Board and will be subject to assessment under the Single Equality Scheme.

17. Links with other policies

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

April ~~2019~~ 2020