DATA PROTECTION POLICY AND PRIVACY NOTICE

April 2022

Created by	Senior Management and Governors
Date	April 2018
Reviewed by	Verity McAuley, SBM / Wendy Perry, HR Manager
Date	April 2022
Ratified by Governors	15 June 2022
Next review date	April 2025

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 that came 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 This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity
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 • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
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.

The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide a regular report of their activities directly to the governors and, where relevant, report their advice and recommendations on data protection issues. The Data Protection Officer is also the first point of contact for individuals whose data the school processes, and for the ICO. Our school delegates the responsibility of data controller to the School Business Manager.

All 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
- Would include another person's personal data that we cannot reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

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. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the Information Commissioner's Office or they can seek to enforce their subject access right through the courts.

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. CCTV

We use CCTV in various locations around the school estate to ensure it remains safe. We will adhere to the Information Commissioner's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Data Protection Officer.

11. 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

12. 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.

13. 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.

14. 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.

15. Data Breaches

We will make all reasonable efforts to ensure that there are no personal data breaches. In the event of a suspected data breach, we will follow the procedure set out in Appendix 1. 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 will 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.

16. The General Data Protection Regulation

We acknowledge that the law has recently changed on the rights of data subjects and that the General Data Protection Regulation has 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.

17. 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.

18. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme, the ICT Acceptable Use policy and the CCTV Policy.

April 2022

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office.

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the Data Protection Officer by emailing veritymcauley@linwood.bournemouth.sch.uk.

The Data Protection Officer will investigate the report and determine whether a breach has occurred. To decide, the Data Protection Officer will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the Data Protection Officer will alert the Executive Headteacher and the Chair of Governors.

The Data Protection Officer will make all reasonable efforts to contain and minimize the impact of the breach. Relevant staff members or data processors should help the Data Protection Officer with this where necessary, and the Data Protection Officer should take external advice when required.

The Data Protection Officer will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

The Data Protection Officer will work out whether the breach must be reported to the Information Commissioner's Office and the individuals affected using the Information Commissioner's Office self-assessment tool.

The Data Protection Officer will document the decisions, in case it is challenged at a later date by the Information Commissioner's Office or an individual affected by the breach.

Where the Information Commissioner's Office must be notified, the Data Protection Officer will do this via the 'report a breach' page of the Information Commissioner's Office website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the Data Protection Officer will set out:

A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Officer
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the Data Protection Officer will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the Data Protection Officer expects to have further information. The Data Protection Officer will submit the remaining information as soon as possible.

Where the school is required to communicate with individuals whose personal data has been breached, the Data Protection Officer will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the Data Protection Officer
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The Data Protection Officer will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The Data Protection Officer will document each breach, irrespective of whether it is reported to the Information Commissioner's Office. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Where appropriate, the Data Protection Officer and Executive Headteacher will investigate and review what happened and how it can be stopped from happening again. This investigation and review will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff who receive personal data sent in error must alert the sender and the Data Protection Officer as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the Data Protection Officer will ask the ICT department/external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the Data Protection Officer will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The Data Protection Officer will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

The Data Protection Officer will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

If safeguarding information is compromised, the Data Protection Officer will inform the designated safeguarding lead and discuss whether the school should inform its local safeguarding partners.