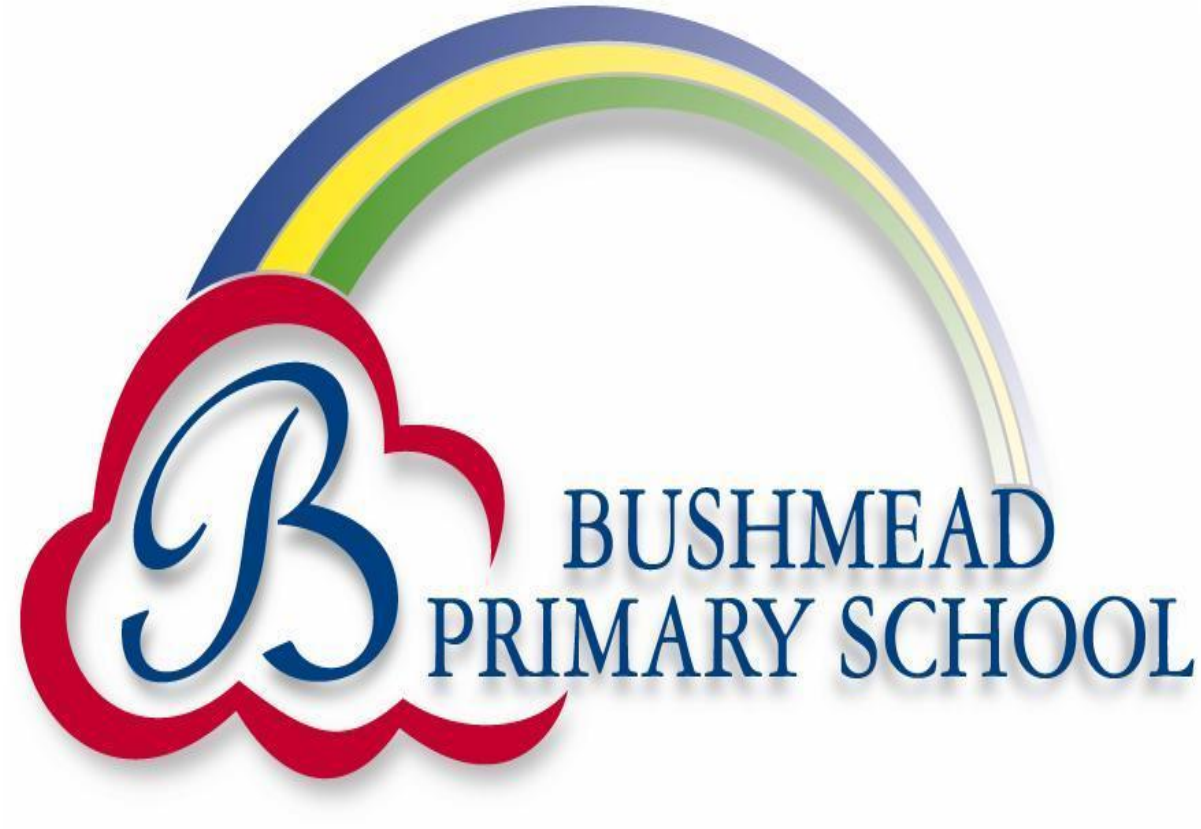
Data Protection POLICY



Owned and Written by	**K Leech** **and Luton Borough Council**	**Date** **September 2022**
Approved by	**Full Governing Body**	**Date** **28/11/22**
Date for Review	**Autumn 2024**	
This policy reflects the General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.		

Contents Page

Introduction

Our school is committed to protecting the rights and freedom of all individuals in relation to the processing of their personal data.

Scope of this policy

This policy has been developed to ensure all staff, contractors and partners understand their obligations when processing personal and special category data in order to comply with the Data Protection Act 2018, The General Data Protection Regulation 2016 and UK General Data Protection Regulations 2021 as amended.

This policy and the legislation apply to all personal data, both that are held in paper files and electronically. So long as the processing of the data is carried out for school purposes, it applies regardless of where data is held.

‘Processing’ data is widely defined and includes obtaining, recording, keeping, or using it in any way; sharing or disclosing it; erasing and destroying it.

Data protection principles

Personal and special category data must be:

- **Processed lawfully, fairly and transparently**
- **Collected for specified, explicit and legitimate purposes**
- **Used in a way that is relevant, adequate and limited to what is necessary**
- **Accurate and, where necessary, kept up to date. Personal data that is inaccurate should be erased or rectified without delay**
- **Kept for no longer than necessary**
- **Kept securely**

Responsibilities of staff and contractors.

Staff and contractors must:

- Complete the Data Protection training as soon as they join the school. This is a mandatory requirement
- Complete an annual refresher course as directed by their manager
- Ensure that they only ever process personal data in accordance with requirements of the relevant legislation
- Follow the 6 Principles highlighted above

Data security

Keeping personal data properly secure is vital in complying with the Data Protection Act. All staff and contractors are responsible for ensuring that any personal data we have access to is kept securely. We are also responsible for ensuring that personal data is not disclosed inappropriately (either orally or in writing or accidentally) to any unauthorised third party.

This includes, as a minimum:

- We should always keep passwords safe and never share them. Follow the guidance on creating safe passwords here. https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email
- Lock away any personal data kept in paper format in a lockable cabinet or pedestal. Do not leave documents on desks unattended at any time
- If it is necessary to take hard copy documents out of the school make sure that those documents are looked after at all times, this includes note books and files. Consider whether it is necessary to take files out of the school at all or if so, take them on an encrypted handheld device or laptop.
- If data has to go onto a ~~disc or~~ memory stick make sure that the device used is encrypted and that the data is password protected.
- If we have access to these devices make sure that they are stored securely and locked away safely when not being used.

Sending personal data securely

We can send documents containing personal data securely using the following methods:

Requested by:	Method:
Hard copy	Documents should be hand delivered to the data subject wherever possible. Check ID and address for sending before handing over documents. Make sure that the documents are securely contained in a sealed envelope. If it is not possible for the data subject to collect the documents themselves, use the **special delivery service** and include the name of the data subject on the envelope to ensure that they sign for the documents. **Note**: Check you have the correct address before posting
Encrypted device	Where the data is especially sensitive consider saving the documents on a password protected, encrypted memory device rather than posting hard copies. The password can be sent to the data subject once they have received the device by post to ensure that only they have access.
Email	**This is the preferred method**. Scan a copy of the file and move it to a secure location on the school's network. Send the file by secure data transfer [currently Egress]. Ask the data subject to confirm receipt of the documents as soon as possible

Data subject rights

Data subjects have defined rights over the use of their data. These rights have been reinforced and extended by the UK GDPR and Data Protection Act 2018.

These rights are:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

The above rights are conditional depending on the reason we hold the data and why we may need to retain it.

Where we have a legal obligation to collect and process data or we are collecting the data to carry out a public task, we cannot always agree with any objection application to the processing of that data. We will consider all requests and explain the reason for the decision.

Similarly if an individual claims that there is an error in the recording of a child protection meeting or a behavioural incident, it is unlikely that these records will be amended because it is likely that the records contain the professional opinion of a social worker or other professional. Whilst the school would be unable to amend the original we would be able to place the individual's objections on file next to the original record so that their objections can be noted.

Where we rely on consent to process data about an individual we will be obliged in most cases to apply the above rights.

Prohibited activities

The following activities are strictly prohibited when processing personal and special category data:

- Sharing passwords to access data
- Sending personal data to a personal email address to work on at home
- Sending data to unauthorised personnel. Always check that the recipients are authorised to view the information being sent
- Sending personal data in an insecure format
- Losing or misplacing personal and sensitive data
- Leaving personal data unprotected
- Accessing information about a pupil or member of staff where there is no legitimate reason for doing do
- Accessing personal data about an individual for personal use
- Disclosing personal data to a third party outside of the school without a lawful basis

Implications of breaching this policy
It is a condition of employment in the case of staff and contractors that they abide by the law and the policies of the school. Any breach of this policy could be considered to be a disciplinary offense and may lead to disciplinary action. A serious breach of the Data Protection Act may also result in the school and/or the individual being held liable in law.

Privacy by Design

Under the Data Protection Act 2018 the School has a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities. In order to achieve this, staff are expected to complete Privacy Impact Assessments to help identify and minimise any data protection risks

Privacy impact assessments (PIA)

The school must do a PIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data on a large scale.
- Use new technologies.
- Carry out profiling on a large scale, including evaluation or scoring of individuals.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.

- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

We must consider completing a PIA when you identify:

- Automated decision-making with significant effects.
- Systematic monitoring.
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

International transfers

Restricted transfers from the UK to other countries, including to the EEA, are now subject to transfer rules under the UK GDPR regime.

There are provisions which permit the transfer of personal data from UK to the EEA and to any countries which are now known as 'adequacy regulations'. There are also provisions which allow the continued use of any EU Standard Contractual Clauses ('SCCs'), both for existing restricted transfers and for new restricted transfers. A Transfer Impact Assessment is now available and is required to be completed if there is a transfer outside of the UK.

Conclusion

Compliance with the Data Protection Act 2018 is the responsibility of all members of staff and contractors. Any questions about this policy or any queries concerning data protection matters should be raised with the Head Teacher.

Definitions

Subject Access Request or SAR	A request for access to data by a living person under the Act is known as a Subject Access Request or SAR. All records that contain the personal data of the subject will be made available, subject to certain exemptions.
Freedom of Information Request or FOI.	A request for access to data held is dealt with under the Freedom of Information Act 2000 and is known as a Freedom of Information Request or FOI. Requests for the data of deceased people may be processed under this legislation.
Personal Data	Personal data means data which relate to a living individual who can be identified directly or indirectly from the data, particularly by ~~e~~ reference to an identifier.

	Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Examples of personal data are the name and address of an individual; email and phone number; a Unique Pupil reference number or an NHS number
Special Category Data	Certain personal data, special category data, is given special protections under the Act because misuse could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Information relating to criminal activities or convictions is not special category data but must be treated with similar safeguards in place. Special category data includes: ● race or ethnic origin of the data subject ● their political opinions ● their religious beliefs or other beliefs of a similar nature ● whether they are a member of a trade union ● their physical or mental health or condition ● their sexual life ● sexual orientation ● Biometrics (where used for ID purposes) ● Genetics
Confidential Data	Data given in confidence or data which is confidential in nature and that is not in the public domain. Some confidential data will also be personal data and/or special category data and therefore come within the terms of this policy. Staff working in social care and in management roles will handle confidential data regularly and must be careful not to disclose this information incorrectly.
Data Controller	The organisation which determines the purposes and the manner in which, any personal data is processed is known as the data controller. The School is the data controller of all personal data used and held by the school.
Data Processors	Organisations or individuals who process personal data on behalf of the data controller are known as data processors. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
Data Subject	A living individual who is the subject of personal data is known as the data subject. This need not be a UK national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject, wherever his nationality or residence.
Lawful Basis	The grounds specified by the Regulations which need to be satisfied for any data processing to be legal. One ground needs to exist for processing personal data. Where special category data is processed a second ground must also exist.

Relevant Professional	The practitioners who supply information held on Social Services records, and various other medical and educational records. A relevant professional will consider where disclosure is likely to cause serious physical or mental harm to the applicant or any third party.
Data Breach	A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A data breach may occur by accidentally sending an email to the wrong person or leaving a file in a public place. Breaches which result in a high risk to the individual must be reported to the ICO within 72 hours.