Three Bridges Primary School

Data Protection Policy

Approval Date: **October 2017**

Review Date: **October 2027**

Headteacher: ……

Data Protection Policy

Purpose

This policy sets out how Three Bridges Primary school collects, uses, and protects personal data. The school is committed to ensuring that personal information about pupils, parents, staff, and others is handled responsibly and in accordance with data protection law.

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 **Z6539174**. This registration is renewed annually and up dated as and when necessary.

Aim

This Policy will ensure that:

- 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 will be aware of their duties and responsibilities under this policy.
- The data protection rights of those involved with the School community are safeguarded.
- There is confidence in the School's ability to process data fairly and securely.

Scope

This Policy applies to all staff, governors, volunteers, contractors, and anyone else who handles personal data on behalf of the school.

It covers all personal data – held electronically, on paper, or recorded in any other format.

Legal Framework

This policy is based on the following legislation and guidance:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018**
- Guidance from the **Information Commissioner's Office (ICO)**
- The **Education (Pupil Information) (England) Regulations 2025**

Definitions

- **Personal Data:** any information relating to an identified or identifiable individual e.g. name, address, pupil number.
- **Special Category Data:** sensitive data such as health, ethnicity, or religion.
- **Processing:** any operation performed on personal data collection (collection, storage, sharing etc.)
- **Data Subject:** the individual whose personal data is being processed.
- **Data Controller:** the school which determines how and why personal data is processed.

The Data Protection Principles

The School will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Stored as long as necessary.
6. Kept secure.

Data Collection and Use

The school collects personal data to:

- Support pupil learning and wellbeing
- Monitor progress and assess achievement
- Provide pastoral care
- Comply with legal obligations (e.g. safeguarding, reporting to authorities)
- Manage staff employment
- Communicate with parents and carers

Personal data will only be used for these purposes unless the individual gives consent for another use.

Data Sharing

The school may share personal data with:

- The local authority
- The Department of Education (DfE)
- Ofsted
- Health and social care services
- Examination bodies
- Other schools (for transition purposes)
- External providers (e.g. school photographers, online learning platforms)

All data sharing will be done securely and in line with legal requirements.

The School will have in place a process for dealing with the exercise of the following rights by Governors, staff, students, 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 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.

Data Retention

Personal data is retained as long as necessary for its purpose. The school follows the **Information and Records Management Society (IRMS)** retention schedule for schools

Roles and Responsibilities

- **Governing Body:** ensure the school complies with data protection laws.
- **Headteacher:** responsible for implementing this policy.
- **Data Protection Officer (DPO):** Gary Stockton, Deputy Headteacher. Advises the school and monitors compliance.
- **All staff:** must follow this policy and handle personal data responsibly.

Data Storage and Security

- Paper records are kept in locked storage.
- Electronic data is stored on secure systems with password protection
- Staff must not store personal data on personal devices or email accounts.

- Portable devices are password protected and only used when necessary.
- Staff will comply with the Schools Acceptable IT use Policy.
- Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

Data Breaches

- All staff will be aware of and follow the data breach security management process.
- 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.
- Any suspected or actual data breach must be reported immediately to the DPO.
- Serious breaches will be reported (by the DPO) to the **Information Commissioner's Office (ICO)** within 72-hours where required.

Rights of Individuals

All data subjects have the right to:

- Access their personal data (Subject Access Request)
- Request correction or deletion
- Object to procession or restrict how data is used
- Withdraw consent (where applicable)

All requests should be made to the DPO in writing.

Subject Access Requests

Requests for access to personal data (Subject Access Request - SAR) will be processed by the DPO. Those making a Subject Access Request will be charged a fee in accordance with Regulations. Records of all requests will be maintained.

The school will comply with the statutory time limits for effecting disclosure in response to a SAR. The statutory time limit of **one calendar month** will be adhered to; however, this can be extended by an additional two months for complex requests or if multiple requests have been made by the individual.

If the school requires more information to verify the scope of the request, the **clock can be paused**. The clock will only restart once the necessary information has been received.

Fee payment: if the school decides to charge a fee, the time limit does not begin until the fee has been paid. Any fee requested by the school will be reasonable and will be used to cover administrative costs.

Ensuring compliance

- All staff receive annual data protection and information security training via The National College
- All new staff will be trained on the data protection requirements as part of their induction.
- All staff will read the Acceptable IT use Policy.

The School advises students whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the School website.
The School also provides a Privacy Notice to staff which is available on the School website.

The School will ensure Privacy Notices contains the following information:

- Contact Data Controller and Data Protection Officer

- Purpose of processing and legal basis. Retentions period. Who we share data with.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

This policy will be reviewed annually or sooner if required by changes in legislation or best practice.

Appendix A

What staff should do:
DO get the permission of your Line 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 school.
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 of 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 locked away.
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.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to Bromcom is restricted to appropriate staff only and that leavers are removed in a timely manner and that generic user names are disabled.

What staff must not do:
DO NOT leave computers signed in when left unattended.
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.
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.