Brabourne Church of England Primary School
Data Protection Policy
October 2026

Version 4.0

"Through creative and challenging experiences, we inspire our school community to develop resilience, a passion for learning and the courage to pursue our dreams. Within our nurturing environment and beyond, we live out Christian values, enabling all to flourish in the love of God."

Policy Overview

This policy outlines how Brabourne Church of England Primary School (the School) handles personal information in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It explains your rights, how we collect, store, and use data, and the steps we take to protect your information.

GDPR and Data Protection Policy

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

The School as the Data Controller will comply with its obligations under the GDPR and DPA and other relevant legislation. The School is committed to being concise, clear and transparent about how it obtains, uses, processes personal information and will ensure data subjects are aware of their rights under the legislation.

All staff shall have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted (processed in general). All staff must read, understand and comply with this policy. All staff will receive annual training on data protection principles and school-specific procedures. The school is committed to a culture of data awareness and continuous improvement.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

What Personal Information does the School Process?
The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

Further information about the data the school processes can be found in our Privacy Notice specific to the data subjects.

The Data Protection Principles
The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation
Personal data will only be transferred to a separate organisation outside the UK where: (a) the transfer is covered by UK adequacy regulations; (b) appropriate safeguards are in place and the School has determined, acting reasonably and proportionately, that the protection following the transfer will not be materially lower than the protection provided under UK data protection law; or (c) an applicable statutory exception applies. Staff must consult the DPO before making or materially changing an international transfer.
This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons regulated under GDPR. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the UK.

Lawful Basis for processing personal information
Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected and explained with practical examples and reasons relevant to each processing activity:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school

- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.
The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information
Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
    a. the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
    b. the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
    c. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    d. the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    e. the processing relates to personal data which are manifestly made public by the data subject
    f. the processing is necessary for the establishment, exercise, or defence of legal claims
    g. the processing is necessary for reasons of substantial public interest

h. the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
i. the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

In terms of keeping children safe from online harm, the School complies with the Age-Appropriate Design Code (Children's Code) and the latest statutory guidance. The School ensures:

- Clear online safety training for pupils, staff, and parents;
- Appropriate filtering and monitoring systems;
- Transparent policies on the use of digital tools;
- A risk management framework addressing issues like grooming, catfishing, and online abuse.

(In terms of keeping children safe from online harm the School is required to comply with the requirements of 'codes of practice' laid out by the regulator.) The School is responsible to provide clear information to children and their parents regarding harmful content that the children may reach via school computers and it must put in place risk management (potential issues children might face eg online malicious behaviours, catfishing, grooming, extremism must be written down) and implement online safety precautions for children. The school should provide training for children about the risks they can face online, these should include educating children on how to communicate with teachers and their parents and share any concerns they have without feeling embarrassed or intimidated.

In addition to the above, the School adheres to the ICO's Children's Code for the protection of online data of under-18s. Online services accessed by pupils will be assessed for risk and reviewed for compliance with the Code's 15 standards, including age-appropriate content, transparency, and default high-privacy settings.

Automated Decision Making
The School does not currently use any automated decision-making systems. If such systems are introduced in the future, the following principles will apply:

- Where the School makes a significant decision about an individual based solely on automated processing (including profiling), it will identify and document an appropriate lawful basis before that decision is made. The School will inform the individual that the decision has been taken by automated means, and will give them the opportunity to make representations about it, request human intervention, and contest the decision.

- Where a significant automated decision would involve special category personal data, it will only be made where an appropriate additional safeguard is in place (for example, the individual's explicit consent).

The School does not currently carry out any fully automated decision-making or profiling that produces legal or similarly significant effects on individuals. If such processing is introduced, the School will update this policy and carry out a Data Protection Impact Assessment (DPIA) to evaluate the risks before doing so.

If an individual asks to challenge or seek reconsideration of an automated decision, staff must contact the DPO immediately, and the School will respond without undue delay.

Data Protection Impact Assessments (DPIA)
All data controllers are required to implement 'Privacy by Design' when processing personal data.
This means the School's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

Documentation and records
Written records of processing activities must be kept and recorded including:
- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

As part of the School's record of processing activities the DPO will document, or link to documentation on:
- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- DPIAs and

- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The School should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

The School conducts an annual information audit to verify the accuracy of its Record of Processing Activities (ROPA), assess changes in data flows, and review third-party contracts. The audit also serves to confirm alignment with the School's Privacy Notices and Retention Schedule.

Privacy Notice

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Privacy notices are reviewed and updated annually. They are available on the school website and provided directly to data subjects or parents/carers, depending on age and context.

The School will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes. Follow this link to the GDPR page on KELSI where you will find the model privacy notice(s) for schools to use:

http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/the-general-data-protection-regulation-gdpr

Individual Rights
Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Appendix 1 - Procedure for Access to Personal Information)*
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- Where applicable, to receive information about a significant decision made solely through automated processing, make representations about the decision, obtain human intervention and contest the decision
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court. Individuals also have a right to make a data protection complaint directly to the school. The School will provide an accessible complaint route (including electronically), acknowledge complaints within 30 days, make appropriate enquiries without undue delay, keep complainants informed of progress, and communicate the outcome without undue delay.

Individual Responsibilities
During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.
If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (eg by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).

- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security
The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical, and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection

- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information

Personal data will be kept securely in accordance with the school's data protection obligations.
Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:

http://www.kelsi.org.uk/__data/assets/word_doc/0012/60213/InformationManagementToolkitforSchools
Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

Data breaches
A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information either by a member of staff or third party;
- Loss of data resulting from an equipment or systems (including hardware or software) failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as a fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams;
- Flagging offences where information is obtained by deceiving the organisation which holds it.

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Staff must use the School's standard Data Breach Reporting Form, available from the DPO, and escalate breaches following the internal reporting flowchart. A central register of all data breaches (including near-misses) is maintained by the DPO and reviewed quarterly to identify patterns or risks requiring mitigation. All data breaches, regardless of severity, must be logged internally and reviewed by the DPO. A formal breach log is maintained for audit and compliance purposes.

Training
The school ensures that all staff receive mandatory annual training on GDPR principles and internal data handling procedures. Induction sessions for new staff include data protection awareness. Refresher courses and updates are provided as needed.

Consequences of a failure to comply
The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.
If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

Review of Policy
This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA and other relevant legislation.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

- **Automated Decision-Making (ADM):** when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. UK data protection law does not generally prohibit automated decision-making. Additional safeguards apply under Articles UK GDPR where there is no meaningful human involvement and the decision produces a legal or similarly significant effect on the individual.
- **Automated Processing:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.
- **Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.
- **Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.
- **Data Subject:** a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.
- **Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.
- **Data Protection Officer (DPO):** the person required to be appointed in public authorities under the GDPR.
- **EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
- **Explicit Consent:** consent which requires a very clear and specific statement (not just action).
- **General Data Protection Regulation (GDPR):** General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.
- **Personal data** is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
- **Personal data breach** means 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.
- **Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

- **Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.
- **Processing** means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.
- **Processor** means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.
- **Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
- **Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.