Be Known. Be Loved. Belong.

"Who you are is God's gift to you. Who you become is your gift to God."

Reepham Church of England Primary School

GDPR Policy

Statement of intent

Reepham Church of England Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the GDPR.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and Reepham Church of England Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

o The General Data Protection Regulation

o The Freedom of Information Act 2000

o The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

o The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

o The School Standards and Framework Act 1998

o Data (Use and Access) Act 2025

This policy will be implemented in conjunction with the following other school policies :

o Online Safety Policy

o Freedom of Information Policy

Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key -coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Principles

a) In accordance with the requirements outlined in the GDPR, personal data will be :

i) Processed lawfully, fairly and in a transparent manner in relation to individuals.

ii) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

iii) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

iv) Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for it is processed, is erased or rectified without delay.

v) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, in order to safeguard the rights and freedoms of individuals.

vi) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

b) The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

Accountability

Reepham Church of England Primary School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

- b) The school will provide comprehensive, clear and transparent privacy policies.
- c) Internal records of processing activities will include the following :
    I. Name and details of the organisation
    II. Purpose(s) of the processing
    III. Description of the categories of individuals and person al data
    IV. Retention schedules (see Record Management Policy)
    V. Categories of recipients of personal data
    VI. Description of technical and organisational security measures

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

o Data minimisation

o Pseudonymisation

o Transparency

o Allowing individuals to monitor processing

o Continuously creating and improving security features

e) Data protection impact assessments will be used, where appropriate.

Data Protection Officer (DPO)

A DPO will be appointed in order to:

i) Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.

ii) Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools, or will be trained in such areas as appropriate.

The DPO will report to the highest level of management at the school, which is the Headteacher.

The DPO will operate independently.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

The school will act as a data processor; however, this role may also be undertaken by other third parties.

Under the GDPR, data will be lawfully processed under the following conditions:

i) The consent of the data subject has been obtained.

ii) Processing is necessary for:

o Compliance with a legal obligation.

The performance of a task carried out in the public interest or in the exercise of official authority

vested in the controller.

For the performance of a contract with the data subject or to take steps to enter into a contract.

Protecting the vital interests of a data subject or another person.

For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.

Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

Processing relates to personal data manifestly made public by the data subject.

Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is
- proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)] , the consent of parents will be sought prior to the processing of their data , except where the processing is related to preventative or counselling services offered directly to a child.

Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

External disks/drives will not be used to hold personal information unless they are password - protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft (including all school iPads , laptops and devices).

Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff must ensure that all personal devices used for accessing school files or email accounts are password protected.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Access to staff emails (via Microsoft) are secured by two-factor authentication.

Circular emails to parents are sent blind carbon copy (BCC), so email addresses are not disclosed to other recipients.

l) Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

o They are allowed to share it.

o That adequate security is in place to protect it.

o Who will receive the data has been outlined in a Privacy Notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

Reepham Church of England Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Headteacher is responsible for the continuity and recovery measures in place to ensure the security of protected data.

Publication of information

Reepham Church of England Primary School has adopted the unamended publication scheme from the Information Commissioner's Office. Information available includes:

o Information on the organisation: locations, contacts and legal governance

o Strategy and performance information

o Decision making processes and consultations

o Policies

o Protocols for delivering our functions (including our curriculum)

o Lists and registers required by law

o The services we offer

Classes of information specified in the publication scheme are made available quickly and easily on request.

Reepham Church of England Primary School will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

Photography

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school will always indicate its intentions for taking photographs or videos of pupils and will retrieve permission before publishing them.

Precautions, as outlined in the Photography and Videos at School Policy, are taken when publishing photographs of pupils, in print, video or on the school website.

Data retention

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS data

All data provided by the DBS will be handled in line with data protection legislation, including electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler .

Date Approved: January 2026

Date for Review: January 2028