



BELMONT PRIMARY SCHOOL

DATA PROTECTION POLICY

2026-2027

Date approved by governors:

Date shared with staff

Date of review: August 2026

Due for review on: August 2027

1. Introduction and Aims

Belmont Primary School collects and uses personal information about pupils, parents and carers, staff and other individuals as part of its day-to-day activities.

The school is committed to protecting personal information and ensuring that it is handled lawfully, fairly, securely and responsibly.

This policy sets out the principles that Belmont Primary School will follow when collecting, using, storing, sharing and disposing of personal data and explains the responsibilities of those who handle personal information on behalf of the school.

This policy aims to:

- ensure that personal data is handled in accordance with data-protection legislation;
- protect the privacy and rights of pupils, families, staff and others whose personal data is held by the school;
- ensure that personal data is collected and used only where there is an appropriate and lawful reason to do so;
- ensure that personal data is accurate, relevant and appropriately protected;
- establish clear responsibilities for the safe and appropriate handling of personal data;
- reduce the risk of loss, unauthorised disclosure or misuse of personal information; and
- ensure that individuals can exercise their rights in relation to their personal data.

2. Scope

This policy applies to all personal data processed by Belmont Primary School, whether held electronically, on paper or in any other form.

It applies to personal data relating to pupils, parents and carers, staff, governors, volunteers, visitors, applicants and any other individuals whose personal information is processed by the school.

The policy applies to all staff, governors, volunteers and others who process personal data on behalf of the school.

All users must handle personal data in accordance with this policy and any associated school procedures, including the school's Computing and Acceptable Use Policy.

Where third-party organisations process personal data on behalf of the school, appropriate arrangements will be put in place to ensure that the information is handled securely and in accordance with data-protection requirements.

3. Data Protection Principles

Belmont Primary School will ensure that personal data is:

- **processed lawfully, fairly and transparently;**
- **collected for specified, explicit and legitimate purposes** and not used in a way that is incompatible with those purposes;
- **adequate, relevant and limited** to what is necessary for the purpose for which it is processed;
- **accurate and, where necessary, kept up to date;**
- **kept for no longer than is necessary;**

- **processed securely**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- managed in a way that enables the school to **demonstrate compliance** with these principles.

Everyone who processes personal data on behalf of the school has a responsibility to support these principles.

4. Roles and Responsibilities

Protecting personal data is a shared responsibility. Anyone who processes personal data on behalf of Belmont Primary School must do so in accordance with this policy and the school's associated procedures.

4.1 Governing Body

The Governing Body has overall responsibility for ensuring that the school complies with its data-protection obligations.

The Governing Body will:

- ensure that appropriate data-protection policies and arrangements are in place;
- provide appropriate oversight and challenge in relation to data protection and information security;
- ensure that the school has access to appropriate Data Protection Officer (DPO) advice and support; and
- review and approve this policy in accordance with the school's policy-review arrangements.

4.2 Headteacher

The Headteacher is responsible for the day-to-day implementation of this policy and for promoting a culture in which personal information is handled appropriately and securely.

The Headteacher will:

- ensure that staff understand their responsibilities when handling personal data;
- ensure that appropriate procedures, training and security arrangements are in place;
- ensure that data-protection concerns and potential breaches are responded to appropriately; and
- seek advice from the DPO where necessary.

4.3 Data Protection Officer (DPO)

The school's DPO provides independent advice and support in relation to data protection.

The DPO will:

- advise the school on its data-protection obligations;
- support the school in monitoring compliance with data-protection requirements;
- provide advice on data-protection risks and Data Protection Impact Assessments (DPIAs) where appropriate;
- advise on the management of personal-data breaches and individual rights requests; and
- act as a point of contact with the Information Commissioner's Office (ICO), where required.

4.4 Staff

All staff who handle personal data are responsible for doing so appropriately and securely.

Staff must:

- access and use personal data only where this is necessary for their role;
- follow this policy and relevant school procedures;
- take reasonable steps to keep personal information accurate and secure;
- not disclose personal information to unauthorised individuals;
- use school-approved systems when storing, accessing or sharing personal data;
- take particular care when handling sensitive or confidential information;
- report suspected data breaches, loss of information or other data-protection concerns promptly; and
- complete relevant data-protection training as required.

4.5 Other Users and Third Parties

Governors, volunteers, contractors and other individuals who are authorised to access personal data must comply with the requirements of this policy appropriate to their role.

Where an external organisation processes personal data on behalf of the school, the school will ensure that appropriate contractual and security arrangements are in place.

5. Collecting and Using Personal Data

Belmont Primary School will only collect and use personal data where there is a clear and legitimate purpose for doing so.

The school will identify an appropriate lawful basis for processing personal data and will only collect information that is necessary and relevant for the intended purpose.

5.1 Informing Individuals

The school will provide clear information about how and why personal data is collected, used, stored and shared, normally through its privacy notices and information provided at the point of collection.

Where information is mandatory, individuals will be informed of this. Where providing information is optional, this will also be made clear.

5.2 Lawful Use of Personal Data

Depending on the circumstances, the school may process personal data because:

- it is necessary to comply with a legal obligation;
- it is necessary to carry out a task in the public interest or exercise official authority;
- it is necessary to fulfil a contract;
- it is necessary to protect someone's vital interests; or
- consent has been given where consent is the appropriate lawful basis.

The school will identify any additional legal basis required when processing special category personal data or criminal offence data.

5.3 Consent

The school will seek consent where consent is the appropriate lawful basis for the activity concerned.

Where the school relies on consent:

- the request for consent will be clear and specific;
- individuals will be given sufficient information to make an informed choice;
- consent will be recorded appropriately; and
- individuals will be able to withdraw their consent.

Withdrawal of consent will not affect processing that has already taken place lawfully.

The school will not seek consent where another lawful basis is more appropriate.

5.4 Using Personal Data for a New Purpose

Personal data will not normally be used for a purpose that is incompatible with the reason for which it was originally collected.

Where the school wishes to use information for a new purpose, it will consider whether this is lawful and compatible with the original purpose and will provide further information to individuals where required.

5.5 Data Minimisation

The school will collect and retain only the personal data that is reasonably necessary for its purposes.

Staff should avoid collecting, copying or retaining personal information simply because it may be useful at some point in the future.

6. Keeping Data Accurate and Secure

Belmont Primary School will take appropriate steps to ensure that personal data is accurate, kept up to date where necessary and protected against unauthorised access, disclosure, loss, damage or misuse.

6.1 Accuracy

The school will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date.

Staff must update records when they become aware that information is inaccurate or incomplete.

Pupils, parents/carers, staff and others will be encouraged to inform the school when relevant personal information changes.

Where inaccurate information has been shared with another organisation or individual, the school will take reasonable steps to notify the recipient of the correction where appropriate.

6.2 Security

Personal data must be stored and handled securely, whether held electronically or on paper.

Staff must:

- use school-approved systems and storage arrangements;
- access personal information only where this is necessary for their role;
- protect accounts, passwords and devices in accordance with the school's Computing and Acceptable Use Policy;
- ensure that personal information cannot be seen or accessed by unauthorised individuals;
- take particular care when sending personal or confidential information electronically;
- keep paper records containing personal information appropriately secure;
- avoid leaving personal information unattended or unnecessarily exposed; and
- dispose of personal information securely when authorised to do so.

6.3 Working Away from School

Where personal data is accessed away from the school site, staff must take appropriate steps to protect its confidentiality and security.

School-approved systems should be used wherever possible, and personal or confidential information must not be stored on personal devices or unauthorised services.

Staff must take particular care when working in public or shared spaces to prevent information being seen, overheard or accessed by others.

6.4 Mistakes and Security Concerns

Staff must report promptly any loss, accidental disclosure, unauthorised access or other concern involving personal data.

This includes information that has been:

- sent or disclosed to the wrong person;
- lost or misplaced;
- accessed by somebody without authorisation;
- stored or shared insecurely; or
- affected by the loss, theft or compromise of a device or account.

Staff should report an honest mistake promptly rather than attempting to conceal or resolve it themselves.

Prompt reporting allows the school to take action to protect individuals and reduce any potential harm.

Suspected personal-data breaches will be managed in accordance with Section 9 of this policy.

7. Sharing and Disclosing Personal Data

Belmont Primary School will only share or disclose personal data where there is a lawful and appropriate reason to do so.

Personal data may be shared with other organisations or individuals where this is necessary for the school's functions, required or permitted by law, necessary to safeguard an individual, or where valid consent has been obtained and consent is the appropriate lawful basis.

7.1 Before Sharing Personal Data

Staff must take reasonable steps to ensure that:

- there is an appropriate reason and lawful basis for sharing the information;
- the recipient is authorised to receive it;
- the identity of the recipient has been appropriately verified where necessary;

- only the information necessary for the purpose is shared;
- an appropriate and secure method of communication is used; and
- a record of the disclosure is made where required.

Where staff are uncertain whether information may be shared, they should seek advice from the Headteacher, DPO or another appropriately authorised member of staff before disclosing it.

7.2 Safeguarding

Data-protection requirements do not prevent the appropriate sharing of information for safeguarding purposes.

Where there is a concern about the safety or welfare of a child, staff must follow the school's safeguarding and child protection procedures and share relevant information with the Designated Safeguarding Lead (DSL) or other appropriate professionals.

Information should be shared in a timely, necessary and proportionate way, with the safety and welfare of the child as the primary consideration.

7.3 Requests from External Organisations

Requests for personal data from external organisations, including public authorities and law-enforcement agencies, will be considered on a case-by-case basis.

The school will take reasonable steps to verify the request and the identity and authority of the person or organisation making it before information is disclosed.

Where necessary, advice will be sought from the DPO or other appropriate professional.

7.4 Publishing Personal Information

Personal data, including photographs and other information about identifiable individuals, will only be published through newsletters, websites, social media or other public communications where there is an appropriate lawful basis and the school's relevant consent, safeguarding and data-protection arrangements have been followed.

Particular care will be taken when publishing information about pupils.

7.5 Data Processors and Service Providers

Where an external organisation processes personal data on behalf of the school, Belmont Primary School will take reasonable steps to ensure that the provider offers appropriate data-protection and security safeguards.

Appropriate contractual arrangements will be put in place where required.

Staff must not introduce new online services, applications or systems involving personal data without following the school's approval arrangements.

8. Individual Rights and Subject Access Requests

Individuals have rights in relation to the personal data held about them. Belmont Primary School will respect these rights and respond to requests in accordance with data-protection legislation.

Depending on the circumstances, these rights may include the right to:

- be informed about how personal data is used;
- access personal data held about them;
- have inaccurate or incomplete information corrected;
- request the deletion of personal data in certain circumstances;
- request that the use of their personal data is restricted in certain circumstances;
- object to certain uses of their personal data; and
- raise a concern about the way their personal data has been handled.

Not all rights apply in every circumstance, and some information may be exempt from disclosure or subject to other legal requirements.

8.1 Subject Access Requests

An individual may request access to personal data that the school holds about them. This is known as a **Subject Access Request (SAR)**.

A request does not have to use the words “Subject Access Request” or be made on a particular form in order to be valid.

Staff who receive a request that appears to be asking for access to personal data must pass it promptly to the Headteacher or other designated member of staff responsible for coordinating the school's response.

The school will:

- record the request and the date it was received;
- take reasonable steps to verify the identity of the requester where necessary;
- clarify the scope of the request where this is reasonably required;
- locate and review relevant personal data;
- consider whether any information is exempt from disclosure or contains personal data relating to another individual; and
- respond within the timescale required by data-protection legislation.

The school will seek advice from the DPO where appropriate.

8.2 Requests Relating to Children

Requests for information about a child will be considered carefully, taking account of the child's age, understanding, rights and the circumstances of the request.

A parent or carer does not automatically have an unrestricted right to access all personal data held about their child.

Where there is uncertainty about whether information should be disclosed, the school will seek appropriate advice before responding.

8.3 Other Requests to Correct or Exercise Rights

Requests to correct inaccurate information or exercise other data-protection rights should be dealt with promptly and referred to the appropriate member of staff where necessary.

Staff must not delete, alter or withhold information simply because a request for access has been received.

9. Personal Data Breaches

A personal data breach occurs where personal data is accidentally or unlawfully lost, destroyed, altered, disclosed or accessed without appropriate authorisation.

Examples may include:

- sending personal information to the wrong person;
- losing paperwork or a device containing personal data;
- accidentally disclosing information about one pupil or family to another;
- unauthorised access to an account, file or system;
- loss or theft of personal information;
- a cyber-security incident affecting personal data; or
- inappropriate sharing, alteration or deletion of personal information.

9.1 Reporting a Suspected Breach

Staff must report any suspected personal data breach **immediately** to the Headteacher or other designated member of staff in accordance with the school's reporting arrangements.

Staff should provide as much relevant information as they reasonably can, including what happened, what information may be affected, who may be affected and any action already taken.

Staff must not attempt to conceal a suspected breach or delay reporting it while trying to resolve the matter themselves.

Prompt reporting will be encouraged. The immediate priority following an honest mistake will be to protect those affected and reduce any potential harm.

9.2 Responding to a Breach

The school will take prompt and proportionate action to:

- contain the breach and prevent further loss or disclosure where possible;
- establish what happened and what personal data is affected;
- identify the individuals who may be affected;
- assess the potential risks and consequences;
- seek advice from the DPO and other relevant professionals where appropriate;
- take appropriate action to reduce the risk of harm;
- record the breach and the action taken; and
- consider whether changes to procedures, systems or training are required.

OneIT will be involved where a breach relates to the school's ICT systems, accounts, devices or cyber-security.

9.3 Notification

Where required by data-protection legislation, the school will notify the Information Commissioner's Office (ICO) of a personal data breach within the required timescale.

Where a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will also inform the affected individual where required.

The decision about whether notification is required will be made following an assessment of the circumstances and, where appropriate, advice from the DPO.

Not every personal data breach requires notification to the ICO.

9.4 Learning from Breaches

Personal data breaches and near misses will be reviewed where appropriate to identify lessons and reduce the likelihood of similar incidents occurring again.

This may result in changes to procedures, technical controls, working practices or staff training.

Deliberate, reckless or repeated failure to follow the school's data-protection requirements may be addressed through the appropriate school procedure.

10. Retention and Disposal

Belmont Primary School will retain personal data only for as long as it is required for the purpose for which it was collected or where there is a legal, regulatory, safeguarding or operational reason for retaining it.

The school will maintain a records retention schedule setting out the retention periods applicable to different categories of information.

Where a specific retention period is required by legislation or statutory guidance, the school will comply with that requirement. Where no statutory period applies, an appropriate retention period will be determined having regard to the purpose of the record, relevant guidance and any potential legal or safeguarding requirements.

10.1 Key Retention Periods

The following table summarises some of the principal retention periods relevant to the school. It is not intended to replace the school's full records retention schedule.

Record	Minimum/Typical Retention
Admission register	6 years from the date of the entry
Attendance register	6 years from the date of the entry
Primary pupil educational record	Retained while the pupil attends the school and transferred securely to the next school when the pupil leaves
Child protection/safeguarding records	Transferred securely to the next school where appropriate; where Belmont is the last known school, retained in accordance with the school's safeguarding retention arrangements, normally until the individual's 25th birthday before review
Records of educational visits	10 years from the date of the visit; records relating to an incident may require longer retention
Accident records	Normally 3 years from the date of the accident; records relating to pupils may need to be retained with the pupil record for longer
Staff personnel files	6 years following termination of employment
Copies of DBS certificates, where retained	No longer than 6 months after the recruitment decision, unless there is a lawful reason for longer retention
Payroll records	At least 3 years from the end of the tax year to which they relate
Contracts	Normally 6 years from the final payment or end of the contractual relationship
VAT and relevant financial records	Normally 6 years from the end of the relevant financial year

Retention periods may be extended where there is a safeguarding concern, ongoing complaint, legal claim, investigation or other legitimate reason why the information must continue to be retained.

The school's full retention schedule will take precedence where a more specific retention requirement applies.

10.2 Transfer of Pupil Records

When a pupil moves to another school, relevant educational and safeguarding records will be transferred securely and promptly in accordance with applicable requirements and guidance.

The school will ensure that particularly sensitive records, including child-protection information, are transferred securely to an appropriate person at the receiving school.

A record of the transfer will be retained where appropriate.

10.3 Secure Disposal

When personal data reaches the end of its required retention period and there is no continuing reason to retain it, it will be disposed of securely.

This may include:

- securely shredding confidential paper records;
- securely deleting electronic records;
- ensuring information held within systems, devices or storage media is appropriately removed; and
- using approved confidential-waste or disposal services where appropriate.

Personal data must not be placed in ordinary waste or otherwise disposed of in a way that could allow unauthorised access.

10.4 Suspension of Disposal

Records must not be destroyed where the school is aware that they may be required in connection with:

- a safeguarding matter;
- a Subject Access Request or other information request;
- a complaint;
- legal proceedings or a potential legal claim;
- an investigation; or
- another matter requiring the information to be preserved.

Normal disposal arrangements may resume once the school is satisfied that there is no longer a requirement to retain the information.

11. Monitoring and Review

The Headteacher has overall responsibility for monitoring the implementation and effectiveness of this policy, with advice and support from the Data Protection Officer (DPO) and other relevant staff or service providers as appropriate.

This policy will be reviewed regularly and at least annually.

The review will take account of:

- changes to data-protection legislation, statutory guidance or regulatory requirements;
- advice or guidance issued by the Information Commissioner's Office (ICO);
- changes to the school's systems, working practices or use of personal data;
- personal data breaches, near misses or identified areas of risk;
- developments in technology that may affect the processing or security of personal data; and
- lessons arising from complaints, requests or incidents.

The policy may be reviewed earlier where there is a significant change to legislation, guidance, school practice or identified risk.

Significant amendments will be approved in accordance with the school's usual governance arrangements.

12. Related Policies and Guidance

This policy should be read alongside other relevant Belmont Primary School policies, procedures and information, including, but not limited to,

- Computing and Acceptable Use Policy;
- Child Protection and Safeguarding Policy;
- Staff Code of Conduct;
- Records Management and Retention Schedule;
- Freedom of Information Policy;
- Business Continuity and Disaster Recovery arrangements;
- privacy notices;
- Subject Access Request procedures;
- personal data breach procedures; and
- any other relevant information-security or records-management procedures.
-

This policy has been developed with regard to:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- relevant Department for Education guidance on data protection and record keeping in schools; and
- guidance issued by the Information Commissioner's Office (ICO).

The school will have regard to updated or replacement legislation and guidance introduced during the lifetime of this policy.