



Barnett Wood Infant School

Data Protection

Policy

2026-27

Barnett Wood Infant School

Policy Impact Statement and Updates

Policy:	Data Protection Policy
Date of review:	June 2026
Governor/s responsible:	James Sutcliffe / Paul Tylor
Status / date of next review:	Annual - June 2027
How well has the policy achieved its purpose and outcomes?	
The primary purpose is to ensure the school complies with data protection laws, particularly the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). It provides clear guidelines for staff on how to handle personal data correctly and securely. The policy aims to protect the rights of individuals (students, staff, parents) regarding their personal data. It helps to mitigate risks associated with data breaches and misuse of personal information. The policy has ensured improved security measures for storing and processing personal data. Staff and governors have a better understanding of their responsibilities regarding data protection. The school community (including parents and students) are clear about how their data is collected, used, and stored and fosters a culture of compliance and data protection awareness throughout the school.	
Updates and/ or changes to policy:	
June 2026	Revised to align with UK GDPR, the Data Protection Act 2018, DfE data protection in schools guidance updated March 2026, DfE generative AI guidance/product safety standards, ICO guidance on SARs and breaches, KCSIE 2025 information-sharing expectations, NCSC password guidance and Data (Use and Access) Act 2025 developments. Summary of changes on p.3
June 2025	Section 3: Added section on Legislation and Guidance No other changes to policy
June 2024	Information Security 5.2 Management information system updated from SIMS to Arbor

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils and or staff with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Barnett Wood Infant School
Data Protection Policy

Key changes at a glance 2026

Area	Previous position / risk	Change made
Legal framework	Policy referred to Data Protection Act 1998 and "Data Protection Act May 2018".	Updated throughout to UK GDPR and Data Protection Act 2018; added reference to DUAA 2025 developments and relevant school guidance.
Data protection principles	Used the old eight Data Protection Act principles, including outdated EEA transfer wording.	Replaced with current UK GDPR principles, including accountability.
Subject access requests	Policy stated 40 calendar days and a £10 fee.	Updated to one month, no usual fee, recognition that SARs may be verbal or written, and limited fee/refusal grounds for manifestly unfounded or excessive requests.
Educational record requests	Included 15 school days but without clear distinction from SARs.	Kept 15 school days for educational record access and clarified interaction with SARs.
Breach management	Simple "report within 72 hours" wording.	Added immediate internal reporting, risk assessment, breach log, ICO notification threshold, 72-hour requirement where notifiable, phased reporting and individual notification for high-risk breaches.
Safeguarding information sharing	Limited explicit link to safeguarding duties.	Added wording from KCSIE expectations that data protection law does not prevent sharing information to keep children safe.
Artificial intelligence	Short AI section and reference to outdated tools.	Expanded to cover unauthorised AI use, approved tools, DPIAs, personal/special category data, safeguarding data, learner-facing products, human oversight and breach reporting.
Cyber security/passwords	Minimum six characters and termly password changes.	Updated to strong unique passwords/passphrases or passwordless methods, MFA for sensitive systems where available/proportionate, access reviews and no routine forced password expiry unless compromise is suspected.
Records retention/disposal	Retention table was very limited.	Expanded retention principles and example categories; added secure disposal requirements for paper and electronic records.
Privacy/accountability	Limited explicit accountability framework.	Added privacy notices, record of processing/information asset register, DPIAs, data sharing agreements, supplier/processor checks and training records.
Photos/videos	Generally sound but brief.	Added consent/preference checks before publication, withdrawal logging, safeguarding checks and periodic review/deletion.

Barnett Wood Infant School
Data Protection Policy

Area	Previous position / risk	Change made
International transfers	Outdated "outside EEA" principle.	Updated to UK GDPR international transfer wording and safeguards.
Supplier management	Not sufficiently explicit.	Added requirements for processor contracts, due diligence, data-sharing documentation and cloud-system assurance.
Training	Limited reference to staff understanding.	Added staff/governor training and awareness expectations covering SARs, breaches, AI, cyber, secure email and safeguarding information sharing.

The Data Protection Officer at the school is – Colin Howard of Satswana DPO Services

Satswana Limited
Suite G12
Ferneberga House
Alexandra Road
Farnborough
Hampshire
GU14 6DQ
01252759177
www.satswana.com
admin@satswana.com

Barnett Wood Infant School DATA PROTECTION POLICY

Contents

1. Introduction.....	6
2. Definitions	6
3. Legislation and Guidance.....	6
4. Data Protection Principles	7
5. Lawful bases for processing.....	7
6. Roles and Responsibilities	8
6.1 Governing Body	8
6.2 Headteacher	8
6.3 Data Protection Officer.....	8
6.4 School Business Manager / office team	8
6.5 All staff, governors, volunteers and contractors	8
7. Accountability, privacy information and records of processing.....	9
8. Individual rights and subject access requests	9
8.1 Subject access requests.....	9
8.2 Educational record requests.....	10
8.3 Other rights requests and complaints.....	10
9. Safeguarding and information sharing	10
10. Data sharing and third-party processors.....	10
11. International transfers.....	11
12. Information security	11
13. Personal data breaches	12
14. Photographs, videos and images.....	12
15. Artificial intelligence (AI)	13
16. Records management, retention and disposal	13
17. Training and awareness.....	14
18. Monitoring and review	14

Barnett Wood Infant School

Data Protection Policy

1. Introduction

Barnett Wood Infant School collects, uses, stores and shares personal data in order to run the school safely and effectively, educate pupils, safeguard children, employ staff, meet statutory duties and communicate with the school community.

The purpose of this policy is to set out how the school complies with UK data protection law and current school guidance, and to provide clear expectations for staff, governors, volunteers and others who process personal data on behalf of the school.

This policy applies to all personal data processed by the school, whether held electronically, on paper, in emails, images, audio/video recordings, online systems, cloud services or any other format.

2. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person, such as a name, pupil record, staff record, contact details, image, identification number, online identifier or combination of information that could identify someone.
Special category data	More sensitive personal data, including information about health, ethnicity, biometric data, religious or philosophical beliefs, trade union membership, sex life or sexual orientation. In a school context this may include medical, SEND, safeguarding or pastoral information.
Criminal offence data	Information about criminal allegations, proceedings, convictions, cautions or related safeguarding/recruitment checks.
Processing	Anything done with personal data, including collecting, recording, storing, using, sharing, adapting, deleting or destroying it.
Data subject	The person the personal data relates to.
Data controller	The organisation that decides why and how personal data is processed. Barnett Wood Infant School is a data controller for most personal data it processes.
Data processor	An organisation that processes personal data on behalf of the school, such as some cloud software providers, payroll providers or IT suppliers.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Legislation and Guidance

This policy has been written with reference to:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Privacy and Electronic Communications Regulations 2003, where relevant.

Barnett Wood Infant School

Data Protection Policy

- Data (Use and Access) Act 2025 and related commencement/guidance updates, where provisions are in force or relevant to school practice.
- Information Commissioner's Office (ICO) guidance, including guidance on subject access requests, personal data breaches, data protection impact assessments, children's data and accountability.
- Department for Education (DfE) data protection in schools guidance and resources.
- DfE guidance on generative artificial intelligence in education and DfE generative AI product safety standards.
- Keeping Children Safe in Education 2025 and the school's safeguarding/child protection arrangements.
- National Cyber Security Centre (NCSC) password and cyber security guidance, and DfE digital and technology standards for schools and colleges.
- The school's related policies, including safeguarding, online safety, acceptable use, cyber security, records retention, freedom of information, complaints, CCTV/photo/video and staff code of conduct policies, where applicable.

4. Data Protection Principles

The school will process personal data in line with the UK GDPR principles. Personal data must be:

1. Processed lawfully, fairly and transparently.
2. Collected for specified, explicit and legitimate purposes and not used in a way that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and, where necessary, kept up to date.
5. Kept in identifiable form for no longer than necessary.
6. Processed securely, using appropriate technical and organisational measures.
7. Processed in a way that allows the school to demonstrate accountability and compliance.

5. Lawful bases for processing

The school will identify and document an appropriate lawful basis before processing personal data.

Depending on the activity, this may include:

- Public task - where processing is necessary for the school to carry out its official functions in providing education and meeting statutory responsibilities.
- Legal obligation - where the school must process data to comply with a legal duty, such as census returns, safeguarding, employment, health and safety or accounting duties.
- Contract - where processing is necessary for employment contracts or contracts with individuals.
- Vital interests - where processing is necessary to protect someone's life.
- Consent - where appropriate, for example some uses of photographs or optional communications. Consent must be freely given, specific, informed and capable of being withdrawn.
- Legitimate interests - where available and appropriate, such as certain processing that is not part of the school's public task. A balancing test will be carried out where needed.

Special category data and criminal offence data will only be processed where a lawful basis and an additional condition under data protection law applies. This may include employment, social security and social

Barnett Wood Infant School
Data Protection Policy

protection law, substantial public interest, health or safeguarding conditions, explicit consent, or the establishment, exercise or defence of legal claims.

6. Roles and Responsibilities

6.1 Governing Body

- Has overall responsibility for ensuring the school meets its data protection obligations.
- Approves this policy and receives assurance that appropriate arrangements are in place.
- Ensures data protection risks, including cyber, safeguarding and AI-related risks, are considered as part of governance.

6.2 Headteacher

- Is responsible for day-to-day implementation of this policy.
- Ensures staff understand their responsibilities and receive appropriate training.
- Ensures data protection is considered when introducing new systems, suppliers, processes or uses of data.
- Works with the DPO and nominated governor to manage risks, requests and incidents.

6.3 Data Protection Officer

The Data Protection Officer is Colin Howard of Satswana DPO Services:

- Satswana Limited, Suite G12, Ferneberga House, Alexandra Road, Farnborough, Hampshire GU14 6DQ.
- Telephone: 01252 759177.
- Website: www.satswana.com.
- Email: admin@satswana.com.

The DPO advises the school on data protection compliance, supports DPIAs, advises on breaches and individual rights requests, and acts as a contact point for the ICO and individuals where appropriate.

6.4 School Business Manager / office team

- Maintain key administrative records and ensure appropriate access controls are applied.
- Support SARs, records management, secure transfers, retention and disposal arrangements.
- Maintain the school's ICO registration/payment and relevant records of processing, with advice from the DPO.

6.5 All staff, governors, volunteers and contractors

- Must only access, use or share personal data where they have a legitimate school reason to do so.
- Must keep personal data secure and confidential.
- Must report any actual or suspected data breach immediately.
- Must follow school policies on acceptable use, email, cloud storage, mobile devices, remote working, photographs/videos and AI.
- Must seek advice from the Headteacher, School Business Manager or DPO where unsure.

Barnett Wood Infant School
Data Protection Policy

7. Accountability, privacy information and records of processing

The school will maintain appropriate records and documentation to show compliance. This includes, where applicable:

- Privacy notices for pupils/parents/carers, staff, governors, volunteers, job applicants and other groups where appropriate.
- A record of processing activities and/or information asset register showing what personal data is held, why it is held, lawful bases, who it is shared with, retention periods and security measures.
- Data protection impact assessments (DPIAs) for new or changed processing likely to present high risk, including new systems, apps, AI tools, biometric systems, CCTV or significant data sharing.
- Data sharing agreements where personal data is shared routinely with another controller.
- Processor contracts and due diligence for suppliers who process personal data on behalf of the school.
- A breach log and records of decisions about whether to notify the ICO or individuals.
- Records of training and staff awareness activities.

8. Individual rights and subject access requests

Individuals have rights over their personal data. These include the right to be informed, right of access, rectification, erasure, restriction, objection, portability where applicable, and rights related to automated decision-making.

8.1 Subject access requests

- A subject access request (SAR) may be made verbally or in writing and does not need to use the words “subject access request”.
- Staff who receive a request that may be a SAR must pass it to the Headteacher or School Business Manager immediately.
- The school will respond without undue delay and normally within one month of receipt. Where the request is complex or numerous requests have been made, the period may be extended by up to a further two months in line with UK GDPR. The requester will be informed where an extension is required.
- The school will make reasonable and proportionate searches for the requested personal data. If more information is needed to identify the individual or clarify the request, the school may ask for it and the response timescale may be paused where permitted.
- The school will not usually charge a fee. A reasonable administrative fee may be charged, or the request may be refused, only where permitted by law, for example where a request is manifestly unfounded or excessive or where further copies are requested.
- Information about other people will be considered carefully and redacted where appropriate unless disclosure is lawful and fair.
- Where a request is made by a parent/carer on behalf of a child, the school will consider the child’s age, understanding, best interests and any safeguarding issues before disclosure.

Barnett Wood Infant School
Data Protection Policy

8.2 Educational record requests

Requests by parents/carers to access a pupil's educational record will be handled in line with the applicable education regulations and will normally be responded to within 15 school days. Where a request also amounts to a SAR, the school will consider both regimes and seek DPO advice where needed.

8.3 Other rights requests and complaints

Requests to correct, delete, restrict or object to processing, or complaints about the way the school handles personal data, should be sent to the Headteacher or School Business Manager. The school will consider requests in line with data protection law and respond appropriately. Individuals can also contact the DPO and have the right to complain to the ICO.

9. Safeguarding and information sharing

Data protection law does not prevent the sharing of information where this is necessary to keep children safe or promote their welfare. Staff must never allow concerns about data protection to delay necessary safeguarding action.

- Staff must share safeguarding concerns promptly with the Designated Safeguarding Lead (DSL) or deputy DSL in line with the school's safeguarding policy.
- The school may share personal data, including special category data, without consent where there is a lawful basis and safeguarding condition to do so, including where seeking consent would place a child at risk or prejudice safeguarding action.
- Safeguarding records will be kept secure, access-limited and transferred separately from the main pupil file when a child moves school, with secure transit and confirmation of receipt.
- Where in doubt, staff should speak to the DSL, Headteacher or DPO. Fears about information sharing must not stand in the way of protecting children.

10. Data sharing and third-party processors

The school may share personal data where lawful and necessary, including with the Department for Education, local authority, safeguarding partners, NHS/school nursing services, police, courts, auditors, payroll/pension providers, insurers, legal advisers, software suppliers and other schools where pupils transfer.

When using suppliers that process personal data on behalf of the school, the school will take reasonable steps to check that the supplier provides adequate security and contractual protections. Processor contracts must include data protection terms required by UK GDPR, including instructions for processing, confidentiality, security, sub-processors, assistance with individual rights and breaches, deletion/return of data and audits/assurance.

Routine data sharing should be documented. New or higher-risk data sharing should be assessed in advance and may require a DPIA or data sharing agreement.

Barnett Wood Infant School
Data Protection Policy

11. International transfers

Personal data will not be transferred outside the UK unless the transfer is permitted under UK GDPR. Where a supplier or system involves international transfers, the school will check that an appropriate transfer mechanism is in place, such as UK adequacy regulations or appropriate safeguards such as the UK International Data Transfer Agreement or UK Addendum, where required.

12. Information security

The school will use appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. Measures will be proportionate to the sensitivity and risk of the data.

- School-owned laptops and portable devices used for personal data must be encrypted where technically possible.
- School computers and laptops must be protected by managed endpoint security/anti-malware and kept updated.
- Accounts must be individual wherever possible; shared accounts should be avoided except where approved and risk-assessed.
- Staff must use strong, unique passwords/passphrases or approved passwordless/passkey methods where available. Passwords should be changed where compromise is suspected or confirmed, not merely because a routine termly change is due.
- Multi-factor authentication must be used for systems holding personal or sensitive data where available and proportionate, especially email, cloud storage, MIS, finance, HR, safeguarding and administrator accounts.
- Access must be limited to those who need it for their role and reviewed periodically, including when staff change role or leave.
- Paper records must be stored securely and locked away when not in use.
- Personal data must not be stored on unencrypted USB drives, unmanaged personal devices or personal cloud/email accounts.
- Remote access and home working must use school-approved systems and must protect confidentiality from family members or others.
- Emails containing sensitive or special category data must be checked carefully before sending and protected by secure transfer methods where appropriate.
- All decommissioned devices and storage media must be securely wiped or destroyed before disposal or reuse.
- Class cameras and memory cards must be kept secure; images must be uploaded only to approved systems and deleted from the device/card when no longer needed.
- Personal data must not be published on the school website, social media or newsletters unless there is a lawful basis and relevant privacy/consent checks have been completed.

Arbor is the school's management information system. Access to Arbor must be role-based and limited to authorised users. The school will seek assurance that cloud systems are appropriately backed up and secured.

Barnett Wood Infant School
Data Protection Policy

13. Personal data breaches

All actual or suspected personal data breaches must be reported immediately to the Headteacher, School Business Manager and/or DPO. Examples include sending personal data to the wrong recipient, losing a device or paper record, unauthorised access to a system, malware/ransomware, accidental publication of personal data, or entering personal/sensitive data into an unauthorised AI tool.

The school will:

- Take immediate steps to contain the breach and protect individuals.
- Record the breach in the school breach log.
- Assess the nature, scope and risks of the breach, including risks to individuals' rights and freedoms.
- Seek advice from the DPO where appropriate.
- Notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach, where the breach is likely to result in a risk to individuals' rights and freedoms.
- Notify affected individuals without undue delay where the breach is likely to result in a high risk to them.
- Review lessons learned and take remedial action, including staff reminders, training, access changes or technical improvements.

If all information is not available within 72 hours, the school may provide information to the ICO in phases, where permitted.

14. Photographs, videos and images

As part of school activities, the school may take photographs or videos of pupils, staff and events. Official school use of images will be managed in line with data protection, safeguarding and online safety requirements.

- The school will explain how photographs and videos may be used, for example on displays, newsletters, the school website, social media, prospectus materials or local press.
- Consent will be sought where consent is the appropriate lawful basis. Consent can be refused or withdrawn at any time. Withdrawal will be logged and future use stopped where practicable.
- Before publication, staff must check current consent/preference records and consider safeguarding risks.
- The school will avoid publishing unnecessary identifying information alongside images of children.
- Parents/carers taking photographs or videos at school events for personal use are not usually covered by data protection law. However, the school will remind them not to share images of other children publicly, including on social media, without the relevant parent/carer's agreement and to consider safeguarding risks.
- Images will be reviewed periodically and deleted when no longer needed.

Barnett Wood Infant School
Data Protection Policy

15. Artificial intelligence (AI)

Generative AI tools and AI-enabled education products can support workload reduction and learning, but they create data protection, safeguarding, accuracy, bias, transparency and security risks. The school will use AI only in a safe, lawful and approved manner.

- Staff, governors, volunteers and pupils must not enter personal data, special category data, safeguarding information, SEND information, assessment data, behaviour records, staff data or confidential school information into unauthorised AI tools or chatbots.
- Any AI tool used for school purposes must be approved by the Headteacher or delegated senior leader, with DPO/IT advice where appropriate.
- A DPIA must be considered before introducing AI tools that process personal data or are used for learner-facing, assessment, safeguarding, monitoring or significant decision-support purposes.
- Staff remain professionally responsible for checking AI-generated content for accuracy, suitability, bias, copyright, confidentiality and safeguarding risk before use.
- AI must not be used as the sole basis for decisions that have legal or similarly significant effects on pupils, parents/carers, staff or applicants.
- Learner-facing AI products must be considered alongside filtering, monitoring, age-appropriateness, safeguarding reporting, SEND needs and product safety standards.
- Any personal or sensitive data entered into an unauthorised AI tool must be treated as a potential personal data breach and reported immediately.

16. Records management, retention and disposal

The school will keep personal data only for as long as necessary for the purpose for which it was collected, taking account of statutory requirements, safeguarding duties, limitation periods and sector retention guidance. The school will maintain a separate records retention schedule or equivalent record which is reviewed periodically.

Record type	Typical retention approach	Notes
Pupil admissions and main pupil file	From application/admission to transfer, then transfer to receiving school where appropriate.	Records must be transferred securely. Retain any residual school copy only where necessary and in line with the retention schedule.
Child protection / safeguarding file	Transfer separately to receiving school as soon as possible and in line with KCSIE expectations.	Secure transit and confirmation of receipt must be obtained. Access must be restricted to those with safeguarding responsibility.
SEND, medical and pastoral records	Retain in line with statutory/sector retention schedule and transfer where appropriate.	Special category data requires additional care and access controls.
Staff personnel file	From appointment until six years after employment ends, unless a	DBS certificates/criminal record information must not be kept longer than necessary; where retained,

Barnett Wood Infant School
Data Protection Policy

	longer period is required for a specific record type or legal reason.	keep only with a valid reason and normally not longer than six months.
Recruitment records for unsuccessful candidates	Retain for the period specified in the retention schedule.	Retain only what is needed to evidence fair recruitment and respond to claims.
Governors	From joining to leaving, with key governance records retained according to the retention schedule.	Governing Body minutes currently retained for 12 years.
Photographs/videos	Keep only while needed for the stated purpose or in line with consent/preference records.	Review periodically and delete when no longer required.
Emails and routine communications	Retain only while needed, then delete or file in an appropriate school system.	Important decisions or records should be saved in the correct system, not left only in inboxes.

Secure disposal must be appropriate to the format and sensitivity of the data. Paper records containing personal data must be cross-cut shredded or disposed of via an approved confidential waste process. Electronic records must be securely deleted, and storage media must be securely wiped or destroyed. Personal data must not be disposed of in ordinary waste or recycling.

17. Training and awareness

- All staff will receive data protection information at induction and regular refresher reminders/training appropriate to their role.
- Training will cover confidentiality, recognising SARs, data breaches, secure email, phishing/cyber risks, safeguarding information sharing, records handling, AI restrictions and use of school systems.
- Governors will receive appropriate information to support oversight of data protection risks and compliance.

18. Monitoring and review

This policy will be reviewed annually or sooner where there are significant changes in law, guidance, school systems, processing activities, cyber risk, AI use or following a serious incident. The next scheduled review is June 2027.

Barnett Wood's ICO Registration Number: Z9028673