



Data Protection Policy

Date Approved	September 2026
Review Date	September 2027
Review Calendar	Annually

Contents

1. Aims and scope
 2. Legislation and guidance
 3. Definitions
 4. Data controller and registration
 5. Roles and responsibilities
 6. Data protection principles
 7. Lawful processing and transparency
 8. Privacy notices and consent
 9. Sharing personal data and safeguarding
 10. Individual rights and subject access requests
 11. Parental access to educational records
 12. Photographs, videos and CCTV
 13. Artificial intelligence, EdTech, filtering and monitoring
 14. Data protection by design and DPIAs
 15. Records of processing, retention and disposal
 16. Data security and international transfers
 17. Personal data breaches
 18. Complaints
 19. Training and awareness
 20. Monitoring and review
- Appendix 1: Personal Data Breach Procedure

1. Aims and scope

Norbury Manor Primary School aims to ensure that personal data relating to pupils, parents and carers, staff, governors, volunteers, visitors and other individuals is collected, used, stored, shared and disposed of lawfully, fairly, transparently and securely.

This policy applies to personal data in any format, including electronic records, paper records, photographs, video, audio, CCTV images and information held within school systems and approved cloud services. It applies to all staff, governors, volunteers, contractors and others who process personal data on behalf of the school.

The school will be able to demonstrate its compliance with data protection law and will keep its policies, procedures, privacy notices, records of processing and associated documentation under regular review.

2. Legislation and guidance

This policy has been updated for the 2026/27 academic year and reflects the current data protection framework in England, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025 (DUAA), which amends and builds on the existing data protection framework

- Privacy and Electronic Communications Regulations (PECR), where applicable
- Education (Pupil Information) (England) Regulations 2005
- Freedom of Information Act 2000, where applicable to information requests
- relevant safeguarding legislation and statutory guidance, including information-sharing duties where necessary to safeguard children

The school also has regard to current Department for Education (DfE) guidance on data protection in schools, privacy notices, artificial intelligence, EdTech, filtering and monitoring, photographs and video, CCTV, record keeping and subject access requests, and to guidance issued by the Information Commissioner's Office (ICO).

Key guidance: [DfE - Data protection in schools](#) | [ICO - Data protection guidance](#)

3. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living person.
Special category data	More sensitive personal data, including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, health, sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, offences or related security measures.
Processing	Any operation performed on personal data, including collecting, recording, organising, storing, viewing, changing, sharing, deleting or destroying it.
Data subject	The individual to whom personal data relates.
Data controller	The organisation that decides why and how personal data is processed.
Data processor	An organisation or person processing personal data on behalf of the controller, other than an employee acting within their duties.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
DPIA	A Data Protection Impact Assessment used to identify and reduce privacy risks, particularly where processing is likely to result in high risk to individuals.
ROPA	The school's Record of Processing Activities, documenting what personal data is processed, why, by whom, for how long and with what safeguards.

4. Data controller and registration

Norbury Manor Primary School is the data controller for most personal data it processes because the school determines the purposes and means of processing. The school will maintain the required registration/data protection fee with the ICO.

5. Roles and responsibilities

Governing Body

The governing body has overall responsibility for ensuring that the school has appropriate data protection arrangements and receives assurance about compliance. It will approve this policy and monitor significant data protection risks.

Data Protection Officer (DPO)

The DPO oversees compliance, advises the school on its obligations, supports DPIAs, monitors data protection practice and training, and acts as a contact point for individuals and the ICO. The DPO must be able to perform these duties independently and report to the highest management level.

The school's DPO is Norma Glaze. Data protection enquiries may be sent to DPO@nmp.croydon.sch.uk.

Headteacher

The Headteacher is responsible for ensuring that this policy is implemented in day-to-day school practice, that staff understand their responsibilities, and that data protection is considered when decisions are made about systems, services and new processing activities.

All staff, governors and authorised users

Everyone handling personal data must:

- process personal data only for authorised school purposes and in accordance with this policy
- keep information accurate, secure and confidential
- use only approved school systems, accounts, devices and services for school personal data unless specifically authorised
- complete required data protection and cyber-security training
- report suspected data breaches immediately to the DPO and follow instructions to contain them
- forward any information-rights request, including a verbal subject access request, promptly to the DPO
- seek advice before starting new processing, using a new system, sharing unusual or sensitive information, or using AI/EdTech where personal data may be involved
- follow the school's retention, disposal, safeguarding, acceptable-use, filtering and monitoring requirements

6. Data protection principles

The school will comply with the UK GDPR principles. Personal data must be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept in identifiable form for no longer than necessary
- processed securely, protecting against unauthorised or unlawful processing and accidental loss, destruction or damage

The school is also responsible for, and must be able to demonstrate, compliance with these principles (the accountability principle).

7. Lawful processing and transparency

Before processing personal data, the school will identify and document an appropriate lawful basis for the activity. The lawful bases include consent, contract, legal obligation, vital interests, public task, and legitimate interests where this is available to a public authority for processing outside its public tasks. The DUAA also

introduced recognised legitimate interests for specified circumstances; the school will only rely on these where the legal conditions are met.

Special category data and criminal offence data require additional conditions under the UK GDPR and Data Protection Act 2018. The school will identify and document those conditions where relevant.

The school will consider whether proposed processing is fair and proportionate and whether individuals would reasonably expect their data to be used in that way.

8. Privacy notices and consent

The school will provide clear and accessible privacy information to individuals whose personal data it processes. Privacy notices will be reviewed at least annually and whenever there is a significant change to the way personal data is collected, used, shared or retained.

The school maintains privacy notices for pupils and parents/carers, the school workforce and governance roles. These will be made freely available, including through the school website where appropriate.

Consent will only be used where it is the appropriate lawful basis. Where consent is relied upon it must be freely given, specific, informed and unambiguous, and the school will keep an appropriate record. Consent may be withdrawn at any time. The school will not seek consent for processing that is required by law or necessary for the school to perform its public functions.

9. Sharing personal data and safeguarding

Personal data will only be shared where there is a lawful basis and a clear purpose. Consent is not required for every disclosure. The school may share information without consent where this is required by law, necessary for a public task, necessary to protect vital interests, or otherwise permitted by data protection law.

Safeguarding information will be shared when necessary, proportionate, relevant, adequate, accurate, timely and secure. Data protection law does not prevent appropriate information sharing to safeguard and promote the welfare of children. Staff must follow the school's safeguarding procedures and consult the DSL and/or DPO where appropriate.

When using processors or contractors, the school will carry out appropriate due diligence, ensure a compliant written contract is in place, share only the data needed for the service, and monitor relevant risks. Data-sharing agreements will be used where appropriate.

10. Individual rights and subject access requests

Individuals have rights in relation to their personal data. Depending on the lawful basis and circumstances, these include rights to be informed, access, rectification, erasure, restriction, data portability, objection, and rights relating to automated decision-making. Where processing relies on consent, consent may be withdrawn.

Subject Access Requests (SARs)

A SAR can be made verbally or in writing and does not need to mention data protection law or use a particular form. Any member of staff who receives a request that appears to ask for an individual's own personal data must forward it to the DPO immediately.

The school may request information that is reasonably necessary to confirm identity or clarify the information requested. The school will respond without undue delay and within the statutory timeframe. Where the law permits an extension, fee or refusal, the school will explain the decision and the individual's right to complain.

Children and SARs

Personal data about a child belongs to the child. When a request is made by a parent or another person on behalf of a child, the school will consider the child's competence, the nature of the information, the child's

wishes and best interests, and whether the requester has authority to act. Competence will be assessed case by case; age alone is not determinative.

The school will consider exemptions and third-party information carefully before disclosure, particularly where safeguarding, serious harm, legal privilege, confidential references or the rights of another person are relevant.

11. Parental access to educational records

As a maintained school, Norbury Manor Primary School will comply with the Education (Pupil Information) (England) Regulations 2005. A pupil's educational record must be made available for a parent to inspect, free of charge, within 15 school days of receiving a written request. A copy must also be provided within 15 school days of a written request, and the governing body may charge no more than the cost of supplying the copy.

This is separate from the child's right of access under data protection law. The school will apply the statutory exemptions, including where information could not lawfully be disclosed to the pupil or disclosure could cause serious harm.

12. Photographs, videos and CCTV

Photographs and videos

Identifiable photographs and videos are personal data. Before taking or using images, the school will identify the purpose and lawful basis, minimise unnecessary personal information, store images securely and ensure use is consistent with the information provided to pupils and parents/carers.

Where the school relies on consent for communication, marketing, publicity or other specified uses, consent choices will be clear and recorded, including through MCAS where appropriate. Consent can be withdrawn. Withdrawal will stop future use based on that consent; the school will take reasonable steps regarding material it controls, while recognising that it may not always be possible to retrieve material already lawfully published or distributed.

The school will consider safeguarding when publishing images and will avoid unnecessary identifying information. Parents/carers taking images for purely personal or household use are generally outside UK GDPR, but the school may set reasonable safeguarding rules for events and may restrict photography where necessary.

CCTV

CCTV is used in locations around the school site for safety, security and safeguarding purposes. The school will ensure that its use is necessary and proportionate, signage is clear, access is restricted, retention is limited, and disclosure is controlled. Requests relating to CCTV footage will be handled under the applicable data protection rules.

13. Artificial intelligence, EdTech, filtering and monitoring

Artificial intelligence (AI)

AI tools can create additional privacy, security, accuracy, bias and safeguarding risks. Staff and pupils must only use AI tools for school purposes in accordance with the school's approved arrangements and any age restrictions or terms of use.

- Personal, special category, safeguarding or confidential information must not be entered into unauthorised AI tools.
- Before an AI tool processes personal data, the school will understand what data the provider collects, how it is used, where it is stored, whether it is used to train models, who it is shared with and what controls are available.

- A DPIA will be completed where processing is likely to result in high risk, including relevant profiling or automated decision-making involving children.
- Human oversight will be maintained for decisions that significantly affect individuals, and the school will comply with the rules on automated decision-making.
- Privacy notices will be updated where the school's use of AI changes how personal data is collected, processed, stored or shared.

Educational technology (EdTech)

Before procuring or adopting EdTech that processes personal data, the school will consider data protection as part of due diligence and procurement. Contracts, security, retention, international transfers, access controls, age appropriateness and supplier use of school data will be reviewed before use.

Filtering and monitoring

The school uses appropriate filtering and monitoring arrangements to help keep pupils safe online. Monitoring may involve the processing of user, device, browsing, alert and account information. Access to alerts and reports will be restricted to authorised staff and handled in accordance with safeguarding, data protection and retention requirements. The school will explain relevant processing in its privacy information and review the privacy impact of new or materially changed monitoring systems.

14. Data protection by design and DPIAs

Data protection will be considered from the start of new projects and throughout the lifecycle of processing. The school will minimise the personal data used, restrict access, apply appropriate retention, use privacy-friendly defaults and build security into systems and processes.

A DPIA will be completed before high-risk processing begins. The DPO will advise on whether a DPIA is required and on the adequacy of proposed safeguards. DPIAs will be kept under review where the nature, scope, context or purpose of processing changes.

15. Records of processing, retention and disposal

The school will maintain appropriate records of its processing activities (ROPA), including categories of data and data subjects, purposes, lawful bases, recipients, retention periods, international transfers where relevant, and security measures.

Personal data will be retained only for as long as necessary. The school will maintain and follow a data retention schedule, review the information it holds, transfer pupil records securely when required, and dispose of records securely when retention periods expire.

Paper records will be confidentially destroyed and electronic records securely deleted or rendered inaccessible. Where a disposal contractor is used, the school will require appropriate security assurances.

16. Data security and international transfers

The school will apply appropriate technical and organisational security measures according to the sensitivity and risk of the information. These include, where appropriate:

- role-based access and least-privilege permissions
- strong authentication, secure passwords and multi-factor authentication where available/required
- encryption of school devices and secure transmission of sensitive data
- secure storage of paper records and clear-desk practices for confidential information
- approved secure methods for remote working and information sharing
- regular software updates, backups, cyber-security controls and recovery arrangements
- appropriate controls for removable media and portable devices
- due diligence and contracts for third-party processors
- prompt removal or adjustment of access when roles change or individuals leave

Personal data must not be stored on personal devices or personal cloud/email accounts unless expressly authorised and appropriately secured. Staff must follow the school's acceptable-use and cyber-security procedures.

Where personal data is transferred outside the UK, the school will ensure a lawful transfer mechanism and appropriate safeguards are in place, taking DPO advice where required.

17. Personal data breaches

All actual or suspected personal data breaches must be reported immediately to the DPO. Staff must not delay reporting while trying to investigate the matter themselves. The school will contain the incident, assess risk, document the breach and decide whether notification is required.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk, affected individuals will also be informed without undue delay unless an exemption applies.

The detailed procedure is set out in Appendix 1.

18. Complaints

The school will provide a clear and accessible route for concerns or complaints about the processing of personal data. Complaints should normally be sent to the DPO at DPO@nmp.croydon.sch.uk. The school will acknowledge, investigate and respond appropriately and keep a record of the outcome.

Individuals also have the right to complain to the Information Commissioner's Office. The school will provide current ICO contact information through its privacy notices and website.

19. Training and awareness

All staff and governors will receive appropriate data protection training as part of induction and refresher training thereafter. Additional training will be provided when legislation, guidance, systems, risks or school processes change. The school will maintain evidence of relevant training and communications.

20. Monitoring and review

The DPO will monitor compliance with this policy and advise the Headteacher and governing body on significant issues. The school will review this policy at least annually and sooner if there are changes to legislation, statutory guidance, technology, school systems or processing activities.

The governing body will approve the policy and receive appropriate assurance about data protection compliance, including significant breaches, risks, training and improvement actions.

Appendix 1: Personal Data Breach Procedure

This procedure applies to any actual or suspected loss, unauthorised access, disclosure, alteration or destruction of personal data.

Immediate action

1. Report the incident immediately to the DPO. If the DPO is unavailable and urgent action is required, inform the Headteacher/Senior Leadership Team.
2. Take proportionate steps to contain the breach without destroying evidence. Examples include recalling an email, disabling a link, recovering a document or device, resetting credentials, restricting access, or asking an unintended recipient to securely delete information.
3. Do not contact the ICO, affected individuals, media or other external bodies on behalf of the school unless authorised. Safeguarding concerns must also be reported through the school's safeguarding procedures.

Assessment and documentation

The DPO will investigate and record:

- what happened and when the school became aware
- the categories and approximate number of individuals affected
- the categories and approximate number of records involved
- the sensitivity of the information and any special category, safeguarding or criminal offence data
- the likely consequences for individuals
- steps already taken and further measures required to contain and mitigate harm
- whether the breach is likely to result in a risk or high risk to individuals' rights and freedoms
- the decision on whether to notify the ICO and/or affected individuals, including reasons

Notification

If notification to the ICO is required, the DPO will make the report without undue delay and, where feasible, within 72 hours of awareness. If all information is not available within that period, the initial report may be supplemented as information becomes available.

Where notification to affected individuals is required, communication will be clear and in plain language and will explain the nature of the breach, likely consequences, steps taken or proposed, and how to obtain further information.

Learning and follow-up

All breaches will be documented, whether or not they are reported to the ICO. The DPO and Headteacher will review significant incidents and trends, identify lessons, and ensure that actions such as process changes, technical controls, contract changes or additional training are completed.

Email and safeguarding information

If sensitive information is sent to the wrong recipient, staff should immediately report it, attempt recall where available, and follow DPO instructions. The school may ask the unintended recipient to delete the information and confirm deletion. Where safeguarding information is compromised, the DSL must be informed promptly so that any safeguarding risk can be assessed alongside the data protection risk.