Data Protection Policy

May 2026-2028
Approved by GB May 2026

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with relevant legislation.

With recent changes to the UK's relationship with the European Union, the policy reflects the UK-GDPR (General Data Protection Regulation) and the Data Protection Act (2018)

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UK- GDPR and DPA 2018. The policy reflects guidance issued by the Information Commissioner's Office (ICO) and Information and Records Management Society.

Please note that from April 2026, the ICO will be known as the Information Commissioner

In addition, the policy sets out good practice issued by the National Cyber Security Centre on the security of electronic data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

The policy covers the following legislation
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees)

Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- Data Access & Use Act 2025 (DUAA)
- Employment Rights Act (1996)

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2025) 'Keeping Children Safe In Education''

This policy will be reviewed and updated in phases as the DUAA provisions come into force. We will monitor ICO guidance and adjust accordingly.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number (or Unique Pupil Number) • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs
	• Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

The Information Asset Owners (IAO) for the school are the governing body.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. In addition, any member of staff who reports another member of staff violating the data protection principles is protected by the schools' Whistleblowing Policy.

5.1 Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations. It is recommended that a member of the governing body is given the role to oversee data protection compliance. Data protection should be an agenda item at every full governors meeting, so the school's compliance can be reviewed.

5.2 Data protection officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Mr Tim Pinto from The E-Safety Office Ltd and is contactable via the School Office.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis. Some of the tasks related to this may be delegated to other members of staff.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data to a 'third country'
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK - GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK-GDPR and Data Protection Act 2018.

The school uses a number of online services to support the teaching and learning and safeguarding of children in the school. This falls under the legitimate interests of processing, however some services do need explicit consent and if required we contact parents directly.

We may use some services where the parent has to register their details with a third party company e.g. catering services. On these occasions, the school will highlight the privacy notice of the third party company.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

In addition to existing lawful bases (such as consent, legitimate interests), we may make use of the new lawful basis of recognised legitimate interests (Article 6(1)(ea)) for certain processing (e.g., safeguarding, security, emergency response). Where this is adopted, we will document the rationale and apply appropriate safeguards.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This must be done via secure manner using a cross shredder or secure bin. Any destruction of a large amount of data must be logged by the data protection lead in school.

Paper data that has to be retained for a specific period of time, must be kept in an archived area which has restricted access. Only specific staff are allowed access to this area.

In addition, staff should follow the retention schedule for electronic data and must ensure that they use a file system to ensure that data can be easily accessed.

This will be done in accordance with the Information and Records Management Society's toolkit for schools.

Working with our external DPO, we maintain up-to-date records of processing activities, DPIAs, risk assessments, and algorithmic governance documentation, incorporating the changes introduced by the Data (Use and Access) Act.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

As the UK is now classed as a 'third country' it will ensure that it obtains a Standard Contractual Contract with data processed outside the European Economic Area.

When transferring personal data outside the UK, we will ensure that protections equivalent to or not materially lower than UK standards apply, using safeguards such as standard contractual clauses, binding corporate rules, or other mechanisms.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the school.

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

In some circumstances, the school may ask the data subject to show identification to verify their relationship with a pupil (please see 9.3)

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

For children over the age of 13, an interview will take place with them by a senior member of staff ensuring that they understand the data being requested. A form will be completed which is based on the Gillick principles of maturity, intelligence and understanding.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

We will carry out a reasonable and proportionate search for personal data when responding to a subject access request. If we require clarification or additional information to process a request, we may pause the response time until such clarification is received.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

Individuals wishing to make a complaint about how we handle their personal data should follow the school complaint procedure. If the complainant remains dissatisfied, they may escalate the matter to the Information Commissioner's Office. Please see Appendix I

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred to a third country.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine- readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO (through the school office). If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, may have access to their child's educational record (which includes most information about a pupil that the school holds on their MIS system) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website
- Social media pages *

* Please note that these are third party platforms and if images are shared, parents should be directed to their specific private policies.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the specific photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with their names. See our E-Safety Policy for more information on our use of photographs and videos.

12. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 12 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are required to change their passwords at regular intervals
- Staff remote access to the school's network from a school's device is via an encrypted private network (VPN)
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- Please see the Information Security Policy for further details

14. Artificial Intelligence

The School recognises that Artificial Intelligence (AI) tools may be used to support administrative, educational and operational activities. Any use of AI involving personal data will be lawful, transparent and proportionate, and will comply with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data Access & Use Act 2025. Staff, governors and volunteers must not input personal data, special category data or confidential information about pupils, parents, staff or the School into AI systems

unless the tool has been formally approved, appropriate contractual safeguards are in place, and a Data Protection Impact Assessment (DPIA) has been completed where required.

AI must not be used for automated decision-making about pupils or staff where such decisions produce legal or similarly significant effects, unless explicitly permitted by law and subject to appropriate human oversight. The School will ensure that AI use supports safeguarding, data minimisation and security principles, and that all users receive appropriate guidance and training on the responsible and ethical use of AI.

Please see NHCS's AI Policy for further details.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in the data breach policy. When appropriate, we will report the data breach to the ICO within 72 hours.

16. Safeguarding

The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

· Whether data was shared
· What data was shared
· With whom data was shared
· For what reason data was shared
· Where a decision has been made not to seek consent from the data subject or their parent
· The reason that consent has not been sought, where appropriate

When providing online services that pupils are likely to access, we will consider and apply measures to protect children's data rights, and limit processing to what is appropriate given their lesser awareness of risks.

The school will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

17. DBS Data

All data provided by the DBS will be handled in line with data protection legislation; this includes 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.

18. Training

All staff are provided with data protection training as part of their induction process. Governor can access training through the Local Authority training offer.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated when any changes take place to data protection law. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

20. Links with other policies/documents

This data protection policy is linked to our:

- Freedom of information policy
- Safeguarding Policy
- E-Safety Policy (including Cyber)
- Bring Your Own Device Agreement
- Artificial Intelligence Policy
- Acceptable Use Agreement

Appendix I

Data Protection Complaints Procedure

This can be a standalone policy or included as an appendix in the Data Protection Policy

1. Introduction

This policy sets out the procedure by which the school will manage and respond to data protection complaints in accordance with the UK General Data Protection Regulation (UK-GDPR), the Data Protection Act 2018 Data , and guidance issued by the Information Commissioner's Office (ICO).

The school is committed to ensuring that personal data is processed lawfully, fairly, and transparently. Where concerns are raised, the school will handle complaints promptly, proportionately, and in a manner that promotes trust and accountability.

2. Scope

This policy applies to:

- Pupils and students
- Parents and carers
- Staff and governors
- Applicants, visitors, and third parties

It covers complaints relating to the handling of personal data, including but not limited to:

- Subject Access Requests (SARs)
- Data breaches
- Accuracy of personal data
- Data sharing and disclosure
- Retention and storage of personal data

3. Definition of a Data Protection Complaint

A data protection complaint is any expression of dissatisfaction regarding how the school has processed personal data.

Complaints do not need to:

- Use legal terminology
- Be submitted in writing
- Explicitly reference data protection law

However, general service complaints that do not relate to personal data handling will be managed under the school's standard complaints procedure.

4. How to Make a Complaint

Complaints may be made via:

- Email
- Letter
- In person

The school will ensure that this process is accessible and clearly communicated through:

- Privacy notices
- The school website
- Correspondence relating to data protection rights

5. Roles and Responsibilities

Headteacher / Senior Leadership Team (SLT): Overall responsibility for ensuring compliance

Data Protection Lead (DPL) / Data Protection Officer (DPO): Oversight of complaint handling, advice, and compliance

All staff: Responsible for recognising and escalating complaints appropriately

6. Handling a Complaint

6.1 Acknowledgement

Complaints will be acknowledged without undue delay and, where appropriate, within 30 calendar days

The school will confirm:

- Receipt of the complaint
- The nature of the concern
- Next steps and expected timescales

6.2 Verification

Where necessary, the school will:

- Verify the identity of the complainant
- Obtain evidence of authority if acting on behalf of another individual

The school will ensure that requests for identification are proportionate.

6.3 Investigation

The school will:

- Conduct a fair and impartial investigation
- Review relevant records and systems (e.g. MIS, CPOMS, email)
- Consult relevant staff
- Seek clarification where required

Investigations will begin upon receipt of the complaint and will be conducted without undue delay.

6.4 Communication

The school will:

- Keep the complainant informed of progress
- Provide updates where delays occur
- Offer a clear point of contact throughout the process

6.5 Outcome

Upon completion of the investigation, the school will:

Provide a clear written response
Explain:

- The scope of the investigation
- Findings and reasoning
- Any actions taken

Where no breach is identified, the school will explain how it has complied with data protection law.

7. Escalation and Further Review

If the complainant remains dissatisfied:

- The school may offer an internal review process
- The complainant will be informed of their right to escalate the matter to the Information Commissioner's Office (ICO)

The school encourages individuals to use its internal complaints process before referring matters externally.

8. Record Keeping

The school will maintain records of:

- The complaint
- Correspondence and evidence
- Investigation outcomes
- Actions taken

Records will be retained in accordance with the school's Retention Schedule and UK-GDPR principles.

9. Learning and Improvement

The school will:

- Review complaints to identify trends or recurring issues
- Implement improvements to policies, procedures, and training
- Use outcomes to strengthen data protection compliance

10. Links to Other Policies

This policy should be read in conjunction with:

Data Protection Policy
Freedom of Information Policy
Complaints Policy
IT Security Policy
Safeguarding Policy

11. Review of Policy

This policy will be reviewed annually or in response to:

- Changes in legislation (including the Data (Use and Access) Act)
- ICO guidance updates
- Identified risks or incidents

12. Contact Details

For data protection complaints contact admin@newton-hill.org.uk FAO Tim Pinto