Data Protection and Privacy Policy

1. Introduction

Newheart Learning Limited is committed to all aspects of data protection, ensuring that all personal data relating to staff, pupils, parents, carers, visitors, and any other individuals is collected, stored, and processed in full compliance with the Data Protection Act 2018 (DPA 2018).

2. Legislation and Guidance

This policy is designed to meet the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, drawing on guidance issued by the Information Commissioner's Office (ICO) and DfE (2023) including:

- UK GDPR – the EU GDPR, as incorporated into UK law (with amendments) through *The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020*.
- Data Protection Act 2018 (DPA 2018).
- ICO guidance on the use of surveillance cameras and handling of personal information.
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2023) 'Data protection in schools'
- ICO – Guide to Data Protection (UK GDPR)

3. Data Controller

NewHeart Learning collects, holds, and processes personal data relating to pupils, parents, carers, staff, visitors, and other individuals in accordance with applicable data protection legislation. As such, NewHeart Learning acts as a data controller.

In compliance with legal requirements, NewHeart Learning will register with the Information Commissioner's Office (ICO) prior to the commencement of trading. The ICO registration number is ZB960743.

4. Roles and Responsibilities

This policy applies to all staff employed by NewHeart Learning, as well as to external organisations or individuals working on our behalf. Failure to comply with this policy may result in disciplinary action.

Data Protection Officer (DPO)

The DPO is responsible for overseeing the implementation of this policy, ensuring compliance with data protection legislation, and developing related policies and guidance as required. The DPO will:

- Ensure all staff complete relevant data protection training.
- Manage and respond to any data protection breaches.
- Handle Subject Access Requests (SARs) and Freedom of Information (FOI) requests.
- Serve as the point of contact for individuals whose data is processed by the provision.
- Act as the first point of contact for the Information Commissioner's Office (ICO).

The DPO for NewHeart Learning Limited is **Nicola Klimczuk**, who can be contacted at office@newheartlearning.co.uk.

All employees
All employees are responsible for:

- Collecting, storing, and processing personal data in accordance with this policy.
- Informing the provision of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - For any questions about the operation of this policy, data protection law, data retention, or data security.
    - If they have concerns that this policy is not being followed.
    - If they are unsure whether they have a lawful basis to use personal data in a particular way.
    - When they need to rely on or obtain consent, draft a privacy notice, address a data protection right invoked by an individual, or transfer personal data outside the United Kingdom.
    - In the event of a data breach.
    - When undertaking any new activity that may affect the privacy rights of individuals.
    - If they require assistance with contracts or sharing personal data with third parties.

5. Data Protection Principles

NewHeart Learning is committed to complying with the data protection principles set out under the UK GDPR. These principles require that personal data is:

- Processed lawfully, fairly, and in a transparent manner.
- Collected for specified, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary to achieve the intended purpose.
- Accurate and, where necessary, kept up to date.
- Retained only for as long as necessary to fulfil the purpose for which it is processed.
- Processed in a manner that ensures appropriate security.

This policy explains how NewHeart Learning implements measures and practices to comply with these principles.

6. Collecting Personal Data

Lawfulness, Fairness, and Transparency
NewHeart Learning will only process personal data when we have a lawful basis under UK data protection law. These lawful bases include:

- Processing is necessary to fulfil a contract with the individual, or to take steps requested by the individual before entering into a contract.
- Processing is necessary to comply with a legal obligation.
- Processing is necessary to protect the vital interests of the individual or another person (e.g., to protect someone's life).
- Processing is necessary to perform a task in the public interest or in the exercise of official authority.
- Processing is necessary for the legitimate interests of NewHeart Learning or a third party, provided these are not overridden by the individual's rights and freedoms.
- The individual (or their parent/carer, where appropriate) has given clear and freely given consent.

Special Categories of Personal Data
For sensitive personal data, we will also satisfy one of the special category conditions under data protection law, including:

- Explicit consent from the individual (or parent/carer where appropriate).
- Processing is necessary for employment, social security, or social protection obligations.
- Processing is necessary to protect vital interests where consent cannot be given.
- Data has been made manifestly public by the individual.
- Processing is necessary for legal claims or proceedings.
- Processing is necessary for reasons of substantial public interest as defined in legislation.
- Processing is necessary for health or social care purposes, by a qualified professional or a person bound by confidentiality.
- Processing is necessary for public health purposes, by a qualified professional or a person bound by confidentiality.
- Processing is necessary for archiving, research, or statistical purposes in the public interest.

Criminal Offence Data
For data relating to criminal offences, we will ensure we meet both a lawful basis and a condition under data protection law. Conditions include:

- Consent from the individual (or parent/carer where appropriate).
- Processing is necessary to protect vital interests where consent cannot be given.
- Data has been made manifestly public by the individual.
- Processing is necessary for legal proceedings or legal rights.
- Processing is necessary for reasons of substantial public interest as defined in legislation.

When collecting personal data, we will provide individuals with all information required by data protection law. We will always ensure that our data processing is fair and reasonable, and that personal data is not used in ways that individuals would not reasonably expect or that could cause unjustified harm.

Limitation, Minimisation, and Accuracy

- Personal data will only be collected for specified, explicit, and legitimate purposes, which will be communicated to individuals at the time of collection.
- If personal data is to be used for a new purpose, individuals will be informed and consent will be obtained where necessary.
- Staff must only process personal data that is necessary to perform their roles.
- Data will be kept accurate and up to date, with inaccuracies corrected or erased as appropriate.
- When personal data is no longer required, it must be deleted or anonymised in accordance with the Records Retention Schedule (see Appendix 1).

7. Consent

Consent is defined in UK GDPR Article 4(110 as: '' any freely given, specific, informed and inambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her''.

NewHeart Learning will ensure that:

- Data subjects are given genuine choice and control over how their personal information is used. Where there is no real choice, consent will not be considered freely given and therefore will be invalid.
- Clear and transparent information will be provided about how personal data will be processed before consent is requested. Consent must always be a clear, voluntary, and positive opt-in.
- Consent will normally be sought directly from the individual concerned, rather than from a third party (except in specific circumstances, such as where a legal representative or power of attorney is authorised). Where an individual lacks the capacity to consent, a 'best interests' decision-making process will be followed.
- Consent will be regularly reviewed and refreshed, with re-consent sought at least annually to ensure it remains valid.
- Consent will only be requested where the individual has a genuine choice and full control over whether or not their data is processed. Where another lawful basis for processing is more appropriate, that basis will be relied upon instead of consent.
- Personal data, including photographs, will not be used in newsletters, websites, social media, or other public platforms without explicit consent from the individual. Similarly, personal information displayed within NewHeart Learning (such as certificates or qualifications) will only be published with consent. Routine consents will be captured through NewHeart Learning's data collection processes to avoid repeated requests.
- Individuals must always be provided with the option to opt-in to receiving communications at the point their data is collected. Where marketing or third-party materials are to be distributed to named individuals, a valid opt-in must be obtained. If this is not possible, such materials will not be sent.

8. Direct Marketing

Under section 122(5) of the Data Protection Act 2018, direct marketing is defined as *"the communication (by any means) of advertising or marketing material that is directed at specific individuals."*

NewHeart Learning will not:

- Sell personal data to any third party. However, we may use collected data to help us, as an alternative provision, understand how pupils, parents/carers, staff, and other stakeholders engage with our services, and to inform improvements to the support and education we provide.
- Engage in any form of direct marketing without first obtaining explicit consent from the individual concerned, or unless we can rely on a clear and legitimate business reason under data protection law.

9. Sharing Personal Data

NewHeart Learning will not normally share personal data without consent. However, there are circumstances where sharing may be necessary, including but not limited to:

- Situations where a pupil or parent/carer poses a risk to the safety of staff.
- Liaising with other agencies, where consent will be sought as appropriate.
- Sharing data with suppliers or contractors to enable the provision of services to staff and pupils (e.g., IT support providers).

When sharing data with suppliers or contractors, we will:

- Only engage those who can demonstrate compliance with UK data protection law.
- Establish contracts to ensure personal data is processed lawfully and fairly.
- Limit the shared data to what is necessary for the supplier or contractor to perform their service.

Personal data may also be shared with law enforcement or government bodies where required by law. In addition, data may be shared with emergency services and local authorities to assist in responding to emergencies affecting pupils or staff.

Any international transfers of personal data will be carried out in compliance with data protection legislation.

10. Subject Access Requests and Other Rights of Individuals

Subject Access Requests (SARs)

Individuals have the right to request access to personal data held about them. This includes:

- Confirmation that their personal data is being processed.
- A copy of the personal data.
- The purposes of processing.
- The categories of personal data concerned.
- Details of who the data has been, or will be, shared with.
- How long the data will be stored, or the criteria used to determine this.
- The existence of rights to request correction, erasure, restriction, or to object to processing.
- The right to complain to the ICO or another supervisory authority.
- The source of the data, if not obtained directly from the individual.
- Information about any automated decision-making affecting them, and its significance.
- Safeguards in place if personal data is transferred internationally.

Submitting a SAR

- SARs can be made in any form, but written requests help us respond efficiently.
- Provide your name, contact details (address, phone, email), and details of the information requested.
- All SARs received by staff must be immediately forwarded to the Data Protection Officer (DPO).

Children and Subject Access Requests

- Personal data about a child belongs to the child, not the parents or carers.
- Parents or carers may make a SAR on behalf of a child only if the child cannot understand their rights or has consented.
- Children under 12 are generally assumed not to have full understanding, so most SARs from parents/carers may be granted without explicit permission.
- Each child's ability to understand their rights will be assessed individually.

Responding to Subject Access Requests

When handling requests, we will:

- May request two forms of identification.

- May contact the individual to confirm the request.
- Respond without delay and within one month of receipt (or one month after identity verification).
- Provide the information free of charge.
- Extend the response period to three months if the request is complex or numerous, notifying the individual within one month with reasons.

Exceptions:
We may withhold information if disclosure could:

- Cause serious harm to the physical or mental health of the child or another person.
- Reveal abuse or risk of abuse, if disclosure is not in the child's best interest.
- Include another person's personal data that cannot be anonymised without consent.
- Be part of sensitive documents, such as those related to crime, legal proceedings, immigration, confidential references, management forecasts, negotiations, or exam scripts.

Unfounded or excessive requests

- We may refuse or charge a reasonable fee for repetitive or excessive requests.
- Individuals will be informed of the reason and their right to complain to the ICO or enforce their rights through the courts.

Other Data Protection Rights
In addition to SARs, individuals have the right to:

- Withdraw consent for processing at any time.
- Request correction, deletion, or restriction of their personal data.
- Prevent processing for direct marketing.
- Object to processing based on public interest, official authority, or legitimate interests.
- Challenge decisions based solely on automated processing or profiling.
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.

Submitting a request to exercise these rights

- All requests should be submitted to the DPO.
- Staff receiving such requests must forward them immediately to the DPO.

11. Photographs and Videos

We may take photographs or record videos of individuals at our provision as part of everyday activities.

Consent

- We will obtain written consent from parents/carers before taking photographs or videos of their child for purposes such as communication, marketing, or promotional materials.
- We will clearly explain to both parents/carers and pupils how the images or videos will be used.
- Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the relevant photographs or videos and ensure they are no longer distributed.

Parents/Carers Taking Photos or Videos

- Photographs or videos taken by parents/carers at provision events for personal use are not covered by data protection law.
- For safeguarding reasons, we ask that any images or videos containing other pupils are not shared publicly on social media unless all relevant parents/carers have given permission.

How We May Use Photographs and Videos

- Within the provision, for example on notice boards, brochures, and newsletters.
- Outside the provision, for example via external photographers, newspapers, or campaign materials.
- Online, including on the provision website or social media pages.

Safeguarding and Privacy

- When photographs or videos are used, they will not include additional personal information that could identify a child.
- For more details on our approach, see our Safeguarding Policy.

12. Artificial Intelligence (AI)

Artificial intelligence (AI) tools are increasingly accessible, and staff, pupils, and parents/carers may be familiar with generative chatbots such as ChatGPT or Google Bard.

While the provision acknowledges that AI can support pupil learning, it also presents potential risks to personal and sensitive data.

To protect the security of personal and sensitive information:

- No one is permitted to input personal or sensitive data into unauthorised generative AI tools or chatbots.
- Any instance of personal or sensitive data being entered into an unauthorised AI tool will be treated as a data breach, and the provision's personal data breach procedure will be followed.

13. Data Protection Principles

We take steps to ensure that data protection is embedded into all of our processing activities. These measures include:

- Appointing a qualified Data Protection Officer (DPO): Ensuring the DPO has the resources and expertise needed to carry out their responsibilities effectively.
- Limiting data processing: Only collecting and processing personal data that is necessary for each specific purpose, in line with data protection principles and relevant laws.
- Conducting Data Protection Impact Assessments (DPIAs): Assessing high-risk processing activities or the introduction of new technologies, with guidance from the DPO.
- Integrating data protection into documentation: Embedding privacy considerations into internal policies, procedures, this policy, and privacy notices.
- Staff training: Providing regular training on data protection law, this policy, related policies, and other privacy matters, with records of attendance maintained.
- Regular reviews and audits: Testing our privacy measures and ensuring ongoing compliance with data protection requirements.
- Safeguarding international data transfers: Implementing appropriate protections when personal data is transferred outside the UK, where different data protection laws may apply.

- Maintaining processing records:
    - Providing data subjects with the DPO's contact details and clear information about how their personal data is used, via privacy notices.
    - Keeping an internal record of all personal data held, including the type of data, the data subjects, purposes of processing, third-party recipients, any transfers outside the UK and safeguards applied, retention periods, and security measures.

14. Data Security and Storage of Records

We are committed to protecting personal data and keeping it secure from unauthorised or unlawful access, alteration, use, or disclosure, as well as from accidental loss, destruction, or damage. Specifically:

- Secure storage: Paper records and portable electronic devices (e.g., laptops, hard drives) containing personal data are kept locked when not in use.
- Confidential information: Papers containing personal data must not be left on desks, tables, or in areas accessible to others.
- Personal devices: Staff and pupils who store personal data on their own devices must follow the same security procedures as for provision-owned equipment.
- Third-party sharing: When personal data is shared with external organisations, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Only in these circumstances may a member of NewHeart Learning staff remove data subjects records from our premises:

- When a pupil is moving to another provision or back into a mainstream setting.
- Where personal information needs to be taken off site, staff must sign it in and out from the office

15. Disposal of Records

Personal data that is no longer required, or that is inaccurate or out of date and cannot or need not be corrected, will be securely disposed of.

- Paper records will be shredded or incinerated.
- Electronic records will be securely deleted or overwritten.
- We may use a third party to dispose of records on our behalf, in which case we will ensure they provide adequate assurances that they comply with data protection law.

NewHeart Learning retains personal data relating to children and young people only for as long as is necessary to fulfil the purposes for which it was collected, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

16. Bring Your Own Device Guidance

Use of Personal Devices and Portable Media

This typically applies to items such as smartphones, tablets, laptops, and USB memory sticks. Personal data held by NewHeart Learning must not be transferred to a personal device unless:

- The device is protected by a strong password (and encrypted if the data could identify an individual).

- Permission for the transfer has been granted by the NewHeart Learning Data Protection Officer (DPO).
- A clear agreement is in place regarding how long the data may remain on the device.

Such transfers will only take place in exceptional, agreed circumstances where full security and encryption can be guaranteed.
When transferring data from personal devices, a secure channel must always be used. Public Wi-Fi networks must not be relied upon as they may not be secure. All portable devices and removable media (such as laptops and USB drives) must be protected with encryption software.

All staff, pupils, and board members who store personal data on personal devices are required to follow the same security standards that apply to NewHeart Learning owned equipment.

17. Personal Data Breaches

The provision will take all reasonable steps to prevent personal data breaches. If a breach does occur, we will report it to the ICO within 72 hours of becoming aware, where required. Examples of breaches in a provision setting may include, but are not limited to:

- Publishing a non-anonymised dataset online, such as exam results of pupils eligible for the pupil premium.
- Disclosing safeguarding information to an unauthorised person.
- Theft of a school laptop containing unencrypted personal data about pupils.

18. Training and Monitoring

Training
All staff receive data protection training as part of their induction process. Ongoing training and professional development will be provided when changes to legislation or policy make it necessary.

Monitoring
The DPO is responsible for monitoring and reviewing this policy. The policy will be reviewed at least annually and shared with all staff.

19. Links to other policies

This data protection and privacy policy is linked to other policies including:

- Safeguarding Policy
- Staff Code of Conduct
- Onboarding / Referral process
- GDPR / Privacy notice for staff and pupils

Date of last review:	14 February 2026
Date to review:	14 February 2027
Author:	Nicola Klimczuk Head of Business Operations
Signed:	*N Klimczuk*

Appendix 1
Record Retention Schedule

NewHeart Learning recognises its obligations under data protection legislation to ensure that personal data is kept only for as long as necessary for the purpose for which it was collected.

Records will be retained in accordance with legal, regulatory and operational requirements and will be securely disposed of once they are no longer required.

Retention periods are based on guidance from the **Information Commissioner's Office (ICO)**, the **Department for Education**, and other relevant statutory guidance.

Record Type	Description	Retention Period	Secure Disposal
Pupil Records (Main File)	Personal details, admissions, assessments, reports	Until pupil reaches age 25	Secure shredding or permanent deletion
Safeguarding / Child Protection Records	DSL records, referrals, chronologies	Until pupil reaches age 25 (or longer if required by law)	Secure shredding or permanent deletion
Attendance Records	Registers and attendance data	6 years	Secure deletion
Behaviour & Incident Records	Behaviour logs, incident reports	6 years	Secure deletion
Accident & First Aid Records	Accident forms, first aid logs	3 years from date of incident (or until age 25 for pupils)	Secure deletion
Staff Personnel Files	Contracts, appraisals, training	6 years after employment ends	Secure shredding
DBS & Vetting Records	DBS certificate numbers, checks	6 months (certificate not retained)	Secure deletion
Payroll & Financial Records	Pay, tax, pensions	6 years	Secure deletion
Complaints Records	Formal complaints and outcomes	6 years	Secure deletion
CCTV Footage	Security recordings	30 days (unless required for investigation)	Automatic overwrite
Visitor Records	Sign-in books	1 year	Secure shredding

Terminology

Term	Terminology
Personal Information / Personal Data	Any information that relates to an identified or identifiable living person. Examples include: Name (including initials), Identification number, Location data, Online identifiers such as usernames. It can also include details relating to an individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
Special Category of Personal Information / Data	Personal data that is more sensitive and requires greater protection, including information about an individual's: Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Genetic data, Biometric data (e.g., fingerprints, retina or iris scans) when used for identification, Health information – physical or mental, Sexual life or sexual orientation.
Processing	Any operation carried out on personal data, whether automated or manual. This includes collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, sharing, erasing, or destroying data.
Data Subject	The living individual whose personal data is collected, held, or processed.
Data Controller	The person or organisation responsible for deciding why and how personal data is processed.
Data Processor	A person or organisation (other than an employee of the data controller) that processes personal data on behalf of the data controller.
Data Protection Officer	Nominated person responsible for overseeing and monitoring the compliance of their organisations processes in compliance with UK data protection law. They must have the training, knowledge and authority to do so effectively.
Regulatory Authority	This refers to the regulatory authority, such as the Information Commissioner's Office (ICO), which oversees and monitors compliance with all aspects of information governance.
Commissioning Body	The local authority / school responsible for placing the student or commissioning the provision.
Personal Data Breach	Any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.