



Data Protection and Privacy Policy

1. Introduction

NewHeart Learning Limited is committed to protecting the privacy and personal information of pupils, parents/carers, staff, visitors and other individuals whose personal data we process. NewHeart Learning will process personal data lawfully, fairly, transparently and securely and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data-protection legislation.

As an Alternative Provision working with children and young people, NewHeart Learning recognises that it processes personal data that may be particularly sensitive, including information relating to safeguarding, SEND, health, education, behaviour and family circumstances. Appropriate technical and organisational measures will therefore be used to protect personal data and ensure that it is only accessed, used and shared where necessary and lawful.

This policy sets out NewHeart Learning's approach to data protection and the responsibilities of those who process personal data on its behalf.

2. Legislation and Guidance

This policy has regard to applicable data-protection legislation and relevant guidance, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where applicable;
- relevant guidance and codes of practice issued by the Information Commissioner's Office (ICO);
- relevant Department for Education guidance relating to data protection, information sharing and safeguarding; and
- other applicable legislation and statutory guidance governing the processing, sharing, retention and security of personal information.

This policy should be read alongside NewHeart Learning's privacy notices, Records Retention Schedule, safeguarding arrangements and other relevant information-governance policies and procedures.

3. Data Controller

NewHeart Learning Limited determines the purposes and means by which personal data is processed in relation to its own activities and is therefore a data controller for those processing activities.

In some circumstances, NewHeart Learning may process personal data alongside or on behalf of commissioning schools, academies, local authorities or other organisations. The respective data-protection responsibilities of the organisations involved will be determined according to the circumstances and, where appropriate, documented through contracts, data-sharing agreements or other appropriate arrangements.

NewHeart Learning Limited is registered with the Information Commissioner's Office (ICO).

ICO registration number: ZB960743.

4. Roles and Responsibilities

This policy applies to all staff, workers, volunteers and other individuals who process personal data on behalf of NewHeart Learning.

Everyone who handles personal data has a responsibility to comply with this policy, NewHeart Learning's associated procedures and applicable data-protection requirements.

Directors and Senior Leadership

The Directors and senior leadership of NewHeart Learning have overall responsibility for ensuring that appropriate data-protection governance, resources, systems and procedures are in place. They will support a culture in which personal information is handled lawfully, securely and appropriately and ensure that significant data-protection risks are addressed.

Data Protection Lead

NewHeart Learning has appointed a Data Protection Lead (DPL) to coordinate and oversee its day-to-day data-protection arrangements.

The Data Protection Lead will:

- provide advice and guidance to staff on data-protection matters;
- support the implementation and review of this policy and associated procedures;
- coordinate responses to subject access requests and other requests relating to information rights;
- coordinate the identification, assessment, recording and management of personal data breaches;
- maintain appropriate data-protection records;
- support the completion and review of Data Protection Impact Assessments (DPIAs) where required;
- support appropriate arrangements for data sharing, processors and third-party services;
- coordinate data-protection training and awareness;
- support the review of privacy notices and retention arrangements; and
- act as an appropriate point of contact for the Information Commissioner's Office where required.

The Data Protection Lead for NewHeart Learning Limited is:

Nicola Klimczuk, Head of Business Operations

Email: office@newheartlearning.co.uk

The designation of a Data Protection Lead does not remove the individual responsibilities of staff or the overall accountability of NewHeart Learning Limited as data controller.

All Staff

All staff are responsible for:

- handling personal data only where necessary for their role;
- complying with this policy, relevant privacy and security procedures and staff training;
- ensuring personal information is accurate and appropriately protected;
- accessing personal data only where they have an authorised reason to do so;
- not sharing personal information with unauthorised persons;
- seeking advice from the Data Protection Lead where they are unsure about the lawful or appropriate use of personal information;

- immediately reporting actual or suspected personal data breaches, loss of information or security incidents;
- consulting the Data Protection Lead before introducing new systems, technologies or processing activities that may present a significant privacy risk; and
- completing required data-protection training.

5. Data Protection Principles

NewHeart Learning will comply with the data-protection principles contained within the UK GDPR. Personal data will be:

- **processed lawfully, fairly and transparently;**
- **collected for specified, explicit and legitimate purposes** and not further processed in a manner incompatible with those purposes;
- **adequate, relevant and limited** to what is necessary for the purposes for which it is processed;
- **accurate and, where necessary, kept up to date**, with reasonable steps taken to correct or delete inaccurate information;
- **kept for no longer than is necessary** for the purposes for which it is processed; and
- **processed securely**, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

NewHeart Learning is also responsible for demonstrating compliance with these principles. Appropriate policies, procedures, records, training, contracts, risk assessments and other accountability measures will therefore be maintained.

6. Collecting and Processing Personal Data

Lawfulness, Fairness and Transparency

NewHeart Learning will only collect and process personal data where there is a lawful and legitimate reason for doing so.

Before processing personal data, NewHeart Learning will identify an appropriate lawful basis under UK GDPR. Depending on the circumstances, this may include:

- consent;
- performance of a contract or taking steps before entering into a contract;
- compliance with a legal obligation;
- protection of someone's vital interests;
- performance of a task carried out in the public interest or exercise of official authority, where applicable; or
- the legitimate interests of NewHeart Learning or a third party, where those interests are not overridden by the rights and freedoms of the individual.

The lawful basis relied upon will depend on the purpose and circumstances of the processing. Consent will not be used where another lawful basis is more appropriate or where an individual does not have a genuine choice.

NewHeart Learning will provide appropriate privacy information explaining how and why personal data is processed, the lawful basis relied upon where required, how long information is retained, who it may be shared with and the rights available to individuals.

Special Category Personal Data

NewHeart Learning processes information that may constitute special category personal data, including information relating to health, SEND, disability, ethnicity, religion and other sensitive personal circumstances.

Where special category personal data is processed, NewHeart Learning will identify both an appropriate lawful basis under Article 6 UK GDPR and an applicable condition under Article 9 UK GDPR and/or the Data Protection Act 2018, as required.

Additional safeguards will be applied to sensitive information, including appropriate access restrictions, security and confidentiality arrangements.

Criminal Offence Data

Where NewHeart Learning processes personal data relating to criminal allegations, offences or convictions, it will ensure that an appropriate Article 6 lawful basis and relevant condition under the Data Protection Act 2018 apply.

Criminal offence information will only be accessed, used and shared where necessary and lawful and will be subject to appropriate safeguards.

Data Minimisation and Accuracy

NewHeart Learning will:

- collect only the personal information reasonably necessary for the identified purpose;
- ensure that personal information is relevant and proportionate;
- take reasonable steps to ensure information is accurate and kept up to date;
- correct inaccurate information where appropriate;
- restrict access to those who require the information for an authorised purpose; and
- securely delete or anonymise personal information when it is no longer required, in accordance with NewHeart Learning's retention arrangements.

7. Consent

Where NewHeart Learning relies upon consent as the lawful basis for processing personal data, consent will be freely given, specific, informed and unambiguous and will involve a clear affirmative action.

Consent will only be relied upon where the individual has a genuine choice about whether their personal data is processed.

NewHeart Learning will:

- clearly explain what the individual is consenting to;
- keep appropriate records demonstrating consent;
- avoid combining consent with unrelated matters where this would prevent a genuine choice;
- make it as easy to withdraw consent as it is to give it;
- keep consent under appropriate review; and
- stop processing based on consent where valid consent is withdrawn, unless another lawful basis applies to the processing.

Where a child is involved, NewHeart Learning will consider the nature of the processing, the child's age, understanding and capacity and the respective rights of the child and those with parental responsibility when determining how consent should appropriately be obtained.

Consent will not be used as the default lawful basis for routine educational, safeguarding, contractual or operational processing where another lawful basis is more appropriate.

Separate and specific consent will normally be obtained where appropriate for uses such as identifiable pupil photographs or videos for publicity, marketing, the NewHeart Learning website or social-media channels.

8. Direct Marketing

NewHeart Learning will ensure that any direct marketing activities involving personal data comply with applicable data-protection legislation and the Privacy and Electronic Communications Regulations (PECR), where applicable.

NewHeart Learning will not sell personal data to third parties.

Where consent is required for direct marketing, communications will only be sent where valid consent has been obtained. Individuals will be provided with a clear and straightforward way to withdraw consent or opt out of future marketing communications.

NewHeart Learning may communicate with pupils, parents/carers, commissioners, professionals and other stakeholders about educational, safeguarding, placement, contractual or operational matters where this is necessary and lawful. Such communications are not treated as marketing merely because they are sent electronically.

9. Sharing Personal Data

NewHeart Learning will share personal data where there is a lawful basis for doing so and where the sharing is necessary, proportionate and relevant to the purpose for which the information is required.

Consent is not always required before personal information can be shared. In particular, information may be shared without consent where another lawful basis applies, including where sharing is necessary for safeguarding, compliance with a legal obligation, protection of vital interests, performance of contractual or commissioning arrangements, or another legitimate and lawful purpose.

Depending on the circumstances, NewHeart Learning may share relevant personal information with:

- commissioning schools, academies and local authorities;
- parents/carers and persons with parental responsibility, where appropriate;
- children's social care and safeguarding partners;
- the police and other law-enforcement agencies;
- health and social-care professionals;
- education professionals and other services supporting the pupil;
- examination, awarding or accreditation organisations;
- transport providers where necessary for safe transport arrangements;
- insurers, legal advisers and professional advisers;
- regulators or public authorities where required or permitted by law; and
- suppliers and service providers processing information on NewHeart Learning's behalf.

When deciding whether to share personal information, staff will consider:

- the purpose of the proposed sharing;
- whether there is a lawful basis;
- whether the information is necessary and proportionate;
- whether only the minimum necessary information is being shared;
- whether the recipient is appropriate;
- how the information will be transferred securely; and
- whether the sharing should be recorded.

Safeguarding Information Sharing

Data-protection law does not prevent the sharing of information for the purpose of safeguarding children where sharing is necessary, proportionate and lawful.

Staff must not allow uncertainty about data protection to prevent appropriate safeguarding information from being shared. Where staff are unsure, they should seek advice from the DSL/DDSL and/or Data Protection Lead, provided that doing so does not cause inappropriate delay where a child may be at risk.

Processors and Service Providers

Where another organisation processes personal data on behalf of NewHeart Learning, appropriate due diligence will be undertaken and a compliant written contract or other appropriate agreement will be in place where required.

NewHeart Learning will only provide processors with the personal data necessary to perform the agreed service and will take reasonable steps to ensure appropriate security arrangements are maintained.

International Transfers

Personal data will only be transferred outside the United Kingdom where permitted by data-protection law and appropriate safeguards are in place where required.

10. Subject Access Requests and Other Rights of Individuals

Subject Access Requests (SARs)

Individuals have the right to request access to personal data that NewHeart Learning holds about them, subject to applicable exemptions and restrictions.

A Subject Access Request (SAR) does not have to use a particular form or wording. A request may be made verbally or in writing and staff should forward any request that may constitute a SAR promptly to the Data Protection Lead.

NewHeart Learning may ask the individual to clarify the information they are seeking where this is necessary to respond to the request.

Where NewHeart Learning has reasonable doubts about the identity of the person making the request, proportionate information may be requested to verify identity.

NewHeart Learning will respond to valid requests without undue delay and within the applicable statutory timeframe. Where permitted by law, the response period may be extended for complex or numerous requests and the individual will be informed accordingly.

SARs will normally be dealt with free of charge. A reasonable fee may be charged, or a request may be refused, where permitted by law, including where a request is manifestly unfounded or excessive.

Children and Subject Access Requests

Personal data relating to a child is the child's personal data.

When a parent/carer makes a request for information relating to a child, NewHeart Learning will consider the child's age, maturity, understanding and ability to exercise their own information rights, together with the nature of the information requested and any relevant safeguarding or confidentiality considerations.

There is no automatic right for a parent/carer to access all personal information held about their child solely because they have parental responsibility.

Where appropriate, NewHeart Learning may seek the child's views or consent before disclosing information to a parent/carer.

Third-Party and Sensitive Information

Before responding to a SAR, NewHeart Learning will consider whether the information contains personal data relating to another person or information subject to an applicable exemption.

Information may be redacted, withheld or otherwise restricted where permitted or required by law. Particular care will be taken with safeguarding information and information whose disclosure may cause harm or prejudice the rights of another individual.

Other Information Rights

Depending on the circumstances and lawful basis for processing, individuals may have rights including:

- to be informed about how their personal data is used;
- access to their personal data;
- rectification of inaccurate personal data;
- erasure of personal data in certain circumstances;
- restriction of processing in certain circumstances;
- objection to certain processing;
- data portability where applicable;
- withdrawal of consent where processing relies upon consent;
- rights relating to solely automated decision-making and profiling; and
- the right to complain to the Information Commissioner's Office.

Requests to exercise information rights should be referred promptly to the Data Protection Lead. NewHeart Learning will consider each request in accordance with the applicable legal requirements, as not every right applies in every circumstance.

11. Photographs and Videos

Photographs and video recordings of pupils constitute personal data where an individual can be identified. NewHeart Learning will ensure that photographs and videos are taken, stored, used and shared lawfully and securely.

Educational and Operational Use

Photographs or videos may be used where necessary and appropriate for legitimate educational, assessment, accreditation, safeguarding or operational purposes.

The appropriate lawful basis for processing will depend on the purpose for which the image or recording is being used. Consent will not automatically be relied upon where another lawful basis is more appropriate.

Images used for educational or evidential purposes will be stored securely, accessed only by authorised persons and retained in accordance with NewHeart Learning's retention arrangements.

Publicity, Website and Social Media

NewHeart Learning will normally obtain appropriate consent before using identifiable photographs or videos of pupils for:

- the NewHeart Learning website;
- social-media accounts;
- promotional or marketing materials;
- press or media purposes; or
- other public-facing communications.

Where consent is relied upon, individuals will be informed how the image or recording is intended to be used and consent may be withdrawn for future use.

Withdrawal of consent will not affect processing that was lawful before consent was withdrawn. NewHeart Learning will take reasonable steps to cease future use of the relevant image where consent was the lawful basis.

Safeguarding and Privacy

Staff will consider safeguarding and privacy when taking or publishing photographs or videos. Images will not normally be accompanied by unnecessary personal information that could increase the risk of identification or harm.

Staff must only use NewHeart-approved devices and systems to take, store or share pupil photographs or videos unless specific alternative arrangements have been authorised.

Parents/Carers Taking Photographs

Where parents/carers are permitted to take photographs or videos at NewHeart Learning activities, they will be reminded to respect the privacy of other pupils and families and not to publish identifiable images of other children without appropriate permission.

NewHeart Learning may restrict photography or recording at an activity where this is necessary for safeguarding, privacy or other legitimate reasons.

12. Artificial Intelligence (AI) and AI Enabled Technologies

NewHeart Learning recognises that artificial intelligence, including generative AI and AI-enabled technologies, may provide benefits for education and administration but can also create risks relating to privacy, confidentiality, accuracy and information security.

Staff must only use AI systems for NewHeart Learning purposes where their use has been authorised or approved and is consistent with NewHeart Learning's policies and procedures.

Staff must not enter personal data, special category data, safeguarding information, confidential pupil information or other sensitive NewHeart Learning information into an unauthorised AI system.

Before an AI system is used to process personal data, NewHeart Learning will consider:

- the purpose and necessity of the processing;
- the lawful basis for processing;
- what personal information the system will receive;
- how information is stored, retained and used by the provider;
- whether information may be used to train or improve AI models;
- security and international-transfer arrangements;
- the accuracy and reliability of outputs;
- the need for human oversight;
- risks to children and other vulnerable individuals; and
- whether a Data Protection Impact Assessment (DPIA) is required.

AI-generated information will not be assumed to be accurate. Appropriate human oversight will be maintained where AI is used to support decisions or work involving pupils, staff or other individuals.

Staff remain responsible for checking AI-generated outputs and must not make significant decisions about an individual solely on the basis of an AI-generated output unless such processing has been specifically assessed and is lawful.

Any accidental or unauthorised disclosure of personal or confidential information to an AI system must be reported immediately to the Data Protection Lead as a **potential data-protection incident**. The incident will then be assessed and managed in accordance with NewHeart Learning's personal data breach procedures.

13. Accountability and Data Protection by Design and Default

NewHeart Learning is responsible for demonstrating compliance with data-protection requirements and will maintain appropriate governance and accountability arrangements.

Data protection and privacy will be considered when new systems, technologies, services, processes or projects involving personal data are introduced or significantly changed.

NewHeart Learning will apply data protection by design and by default by:

- limiting the collection and use of personal data to what is necessary;
- ensuring access to personal information is appropriately restricted;
- considering privacy and security when procuring or introducing systems and services;
- maintaining appropriate privacy notices and records of processing activities;
- implementing appropriate contracts and data-processing arrangements;
- reviewing data-sharing arrangements where appropriate;
- maintaining appropriate retention and secure-disposal arrangements;
- providing staff training and guidance;
- periodically reviewing data-protection risks and controls; and
- completing Data Protection Impact Assessments where required.

Data Protection Impact Assessments

A DPIA will be completed where processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA may also be appropriate where NewHeart Learning proposes significant new or changed processing involving, for example:

- new monitoring or surveillance technologies;
- extensive processing of sensitive or safeguarding information;
- new AI or automated technologies;
- systematic monitoring of individuals;
- biometric or other particularly intrusive technologies; or
- other processing presenting significant privacy risks.

The Data Protection Lead should be consulted at an early stage where staff are considering new systems or processing activities involving significant amounts of personal or sensitive information.

14. Data Security and Storage of Records

NewHeart Learning will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Security arrangements will be proportionate to the sensitivity of the information and the risks associated with its processing.

Electronic Information

Personal data held electronically will be stored using NewHeart-approved systems and devices wherever reasonably practicable.

Appropriate security measures will include, where applicable:

- strong passwords and appropriate authentication controls;
- access permissions based on role and operational need;
- encryption and secure transfer methods;
- device locking and screen-locking arrangements;
- appropriate anti-malware, security updates and system maintenance;
- secure backup arrangements;
- restrictions on downloading or locally storing sensitive information; and
- prompt removal of access when staff leave or no longer require it.

Staff must not share passwords or allow unauthorised individuals to access NewHeart Learning systems.

Paper Records

Paper records containing personal or confidential information will:

- be stored securely when not in use;
- not be left unattended where unauthorised individuals could access them;
- only be removed from the provision where there is a legitimate operational reason;
- be transported securely where removal is necessary; and
- be returned to secure storage or securely disposed of when no longer required.

Personal Devices

NewHeart Learning personal data, particularly safeguarding information, special category data and confidential pupil information, must not normally be stored on personal devices.

Where exceptional circumstances require the use of a personal device, this must be authorised in advance by an appropriate senior member of staff/Data Protection Lead and appropriate security arrangements must be in place.

Staff must not use personal email accounts, personal cloud-storage services or unauthorised messaging services to store or transfer NewHeart Learning personal data.

Sharing and Transfer

Personal information will only be transferred using appropriately secure methods having regard to the sensitivity of the information.

Particular care will be taken when sending information electronically to ensure that:

- the intended recipient is correct;
- only necessary information is included;
- attachments are correct;
- sensitive information is appropriately protected; and
- secure transfer methods are used where appropriate.

Access

Access to personal information will be limited to individuals who require it for an authorised purpose. Access permissions will be reviewed and amended where roles or responsibilities change.

15. Retention and Secure Disposal of Records

NewHeart Learning will retain personal data only for as long as it is necessary for the purpose for which it was collected or subsequently lawfully processed, taking account of applicable legal, safeguarding, contractual, commissioning, insurance and operational requirements.

Retention periods will be set out in NewHeart Learning's Record Retention Schedule and will be reviewed periodically.

Where information is no longer required, it will be securely deleted, destroyed or anonymised as appropriate.

Secure disposal methods will include:

- confidential shredding or other secure destruction of paper records;
- secure deletion of electronic records and files;
- appropriate secure disposal or wiping of electronic devices and storage media; and
- appropriate arrangements for information held within third-party systems.

Where a third party is used to dispose of personal data or equipment containing personal data, NewHeart Learning will ensure appropriate contractual, confidentiality and security arrangements are in place.

Records that are subject to an ongoing safeguarding matter, complaint, investigation, legal claim, regulatory enquiry or other legitimate requirement will not be destroyed solely because their usual retention period has expired. They will be retained for as long as reasonably necessary and securely disposed of when no longer required.

16. Personal Devices and Removable Media

NewHeart Learning personal data should be accessed, stored and processed using NewHeart-approved devices, systems and accounts wherever reasonably practicable.

Staff must not routinely download, copy or transfer NewHeart Learning personal data onto personally owned devices, personal email accounts, personal cloud-storage services, personal USB drives or other unauthorised storage media.

Where exceptional circumstances require personal data to be processed using a personally owned device, prior authorisation must be obtained from an appropriate senior member of staff or the Data Protection Lead.

Any authorised use must be subject to appropriate safeguards, which may include:

- strong passwords and device security;
- encryption where appropriate;
- current security updates;
- secure network connections;
- separation of NewHeart Learning information from personal information where practicable;
- restrictions on copying or onward sharing;
- secure deletion once the information is no longer required on the device; and
- immediate reporting if the device is lost, stolen, compromised or accessed without authorisation.

Removable media containing personal data should only be used where necessary and authorised and must be appropriately encrypted or otherwise secured.

NewHeart Learning reserves the right to withdraw permission to use personal devices for work purposes where security or data-protection requirements are not being met.

17. Personal Data Breaches

A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples may include:

- personal information being sent to the wrong recipient;
- loss or theft of a device or document containing personal information;
- unauthorised access to NewHeart Learning systems or records;
- accidental publication or disclosure of personal information;
- loss of access to personal information where this affects its availability;
- inappropriate disclosure of safeguarding or sensitive information; or
- personal or sensitive information being entered into an unauthorised system or AI tool.

Reporting a Breach

Staff must report any actual or suspected personal data breach to the Data Protection Lead **immediately**. Staff must not delay reporting while attempting to determine whether the incident is serious enough to constitute a breach.

NewHeart Learning will promptly assess the incident, including:

- what happened and when;
- the categories and approximate volume of personal data involved;
- the individuals affected;

- the sensitivity of the information;
- the potential consequences for affected individuals;
- whether information can be recovered, contained or protected; and
- what steps are required to reduce the risk of harm.

Appropriate action will be taken to contain and manage the breach and relevant details and decisions will be documented.

Notification to the ICO

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, NewHeart Learning will notify the Information Commissioner's Office without undue delay and, where feasible, within **72 hours of becoming aware of the breach**.

Where a breach is unlikely to result in a risk to individuals' rights and freedoms, notification to the ICO will not normally be required, but the breach and the reasons for the decision will be appropriately recorded.

Notification to Individuals

Where a personal data breach is likely to result in a **high risk** to the rights and freedoms of affected individuals, NewHeart Learning will inform those individuals without undue delay unless an applicable exception applies.

Where appropriate, NewHeart Learning may also notify or consult other relevant organisations, such as a commissioning school or local authority, safeguarding partner, insurer, IT provider or law-enforcement agency.

All personal data breaches and significant data-protection incidents will be recorded and periodically reviewed to identify lessons, recurring risks and improvements required.

18. Training, Monitoring and Compliance

All staff who process personal data will receive appropriate data-protection and information-security training as part of their induction.

Refresher training and updates will be provided periodically and where appropriate following significant changes to legislation, guidance, technology, NewHeart Learning procedures or identified risks.

Additional guidance or training may be provided to individuals whose roles involve significant responsibility for personal, special category, safeguarding or other confidential information. Staff are expected to comply with this policy and associated data-protection and information-security procedures. Serious or deliberate breaches may be dealt with under relevant disciplinary procedures.

The Data Protection Lead, supported by senior leadership, will monitor the implementation of this policy and may undertake periodic checks, reviews or audits of data-protection arrangements. Lessons arising from personal data breaches, complaints, Subject Access Requests, DPIAs, safeguarding matters, audits and other incidents will be considered when reviewing NewHeart Learning's data-protection arrangements.

19. Links to other policies

This policy should be read alongside other relevant NewHeart Learning policies, procedures and notices, including, where applicable:

- Safeguarding Policy;
- Online Safety Policy;
- CCTV Policy;
- Staff Code of Conduct;
- Complaints Policy;
- referral and placement procedures;
- Records Retention Schedule;
- personal data breach procedures;
- privacy notices for pupils, parents/carers, staff and other relevant individuals; and
- relevant IT, information-security and acceptable-use arrangements.

The Data Protection Lead will coordinate the review of this policy, supported by senior leadership.

The policy will be reviewed **at least annually** and sooner where necessary following:

- significant changes to data-protection legislation or regulatory guidance;
- changes to NewHeart Learning's systems, technology or processing activities;
- significant data breaches or information-security incidents;
- findings from audits, DPIAs, complaints or investigations; or
- significant changes to NewHeart Learning's operating or commissioning arrangements.

Date of last review:	30 August 2026
Date to review:	30 August 2027
Author:	Nicola Klimczuk Head of Business Operations
Signed:	<i>N Klimczuk</i>

Appendix 1

Record Retention Schedule

NewHeart Learning retains records only for as long as they are required for the purpose for which they were created or subsequently lawfully processed, taking account of applicable legal, safeguarding, contractual, commissioning, insurance and operational requirements.

NewHeart Learning is a non-school Alternative Provision and may receive information from commissioning schools, academies, local authorities, parents/carers and other professionals. The fact that information forms part of a pupil's wider education record does not necessarily mean that NewHeart Learning is required to retain the statutory or permanent pupil record.

Where NewHeart Learning holds copies of information for the purpose of delivering an Alternative Provision placement, those copies will be retained only for as long as NewHeart Learning has a lawful and operational need for them.

Where NewHeart Learning creates substantive records relating to its own provision, safeguarding activity, incidents, assessments, interventions, complaints or other activities, these will be retained in accordance with the schedule below.

Retention periods may be extended where information is required for an ongoing safeguarding matter, complaint, investigation, legal claim, insurance matter, regulatory or commissioner enquiry or other legitimate reason. The reason for any extended retention should be recorded where appropriate.

At the end of the applicable retention period, records will be securely destroyed, deleted or anonymised unless there is a lawful reason for continued retention.

Record type	Recommended NewHeart retention
AP pupil/placement file – referral, placement agreement, PLP, assessments, reports, progress and provision records	6 years after the placement ends, unless longer retention is justified
Copies of EHCPs, school reports and information supplied by commissioners	Duration of placement + reasonable closure period, normally then securely delete where the originating organisation retains the substantive record, unless continued retention is necessary
Safeguarding/child-protection records created by NewHeart	Retain securely in accordance with safeguarding record-retention requirements and case circumstances; do not routinely destroy simply when the placement ends
Attendance/session records	6 years after the end of the placement
Behaviour and incident records	6 years after the end of the placement, subject to longer retention where linked to safeguarding, injury, complaint or legal matter
Physical intervention/restraint records	6 years after the pupil's placement ends, or longer where safeguarding, injury, complaint or legal considerations require
Accident/first-aid records	Retain in accordance with applicable health and safety/legal requirements and limitation

Record type	Recommended NewHeart retention considerations; longer where the incident involves a child or could give rise to a claim
Medication/medical administration records	Normally 6 years after the end of the placement, with longer retention where an incident/claim/safeguarding matter requires
AQA/qualification/assessment evidence	According to awarding-body requirements and NewHeart's operational need; unnecessary copies should then be securely deleted
Complaints and outcomes	6 years after complaint closure, longer where safeguarding/legal issues require
Pupil/parent consent records	Duration of relevant processing/activity plus sufficient period to demonstrate the consent relied upon, normally linked to the relevant record's retention period
Staff personnel files	6 years after employment ends, unless a longer period is justified
Recruitment records – unsuccessful applicants	Normally 6 months after recruitment concludes, unless there is a justified reason to retain longer
DBS certificates	Do not routinely retain copies. Normally no longer than 6 months where temporary retention is necessary; retain appropriate details of the check instead
Single Central Record / safer recruitment checking records	Maintain while relevant; historical information retained where necessary to evidence safer recruitment and employment decisions
Staff safeguarding/allegation records	Retain according to applicable safeguarding/allegation record-retention requirements rather than the ordinary personnel-file period
Payroll, tax and financial records	Normally at least 6 years, subject to applicable HMRC/accounting requirements
Contracts and commissioning records	Normally 6 years after contract/placement arrangements end, longer where contractual/legal requirements apply
CCTV footage	Normally 30 days, unless footage is required for safeguarding, investigation, complaint, legal proceedings or another legitimate purpose
Visitor records	Normally 1 year, unless required for safeguarding, investigation or another legitimate purpose
Data breach records	Normally 6 years from closure, subject to the circumstances and continuing legal/regulatory need
DPIAs and significant data-protection decision records	For the lifetime of the relevant processing/activity and an appropriate period afterwards

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 Lead	The person appointed by NewHeart Learning to coordinate and support its data-protection arrangements, including providing guidance, supporting information-rights requests, data-breach management, DPIAs, training and compliance monitoring. The role does not constitute the appointment of a statutory Data Protection Officer unless NewHeart Learning specifically determines that such an appointment is required.
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.