The NEST alternative provision

Data Protection Policy

Date written:	September 2025
Written by:	Joy Iliff
Date reviewed:	-
Reviewed by:	-
Approved on:	October 2025
Review date:	September 2026
Substantive changes since last review:	-

Contents

Policy aims

The NEST has an obligation as a data controller (registered with the Information Commissioner's Office) to ensure legal compliance with the processing of personal data for learners, caregivers, staff, commissioners, visitors, collaborators and suppliers. We respect people's right to privacy, and we will treat it with the same level of conscientiousness as we would treat our own individual personal data. We support data subjects' access to their data and right to correct errors. Data breaches will be treated seriously and reported to the ICO as necessary. We will work with the ICO to protect data. For ecological reasons we aim to minimise physical copies of paperwork. However, there are circumstances in which physical copies must be kept (such as fire lists), this policy applies to both digital and physical storage. Technical and organisational measures are employed to ensure that by default personal data is protected.

Data Protection Officer: Aoife Healy, aoife@thenest-ed.uk

The NEST takes every precaution we can to ensure that data is:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, limited to what is necessary for the stated purpose
- Accurate and kept up to date
- Kept for no longer than necessary for the purpose of collection
- Securely stored and processed
- Only shared with third parties who have read, understood and agreed to this policy
- Not used in any automated decision-making since it is antithetical to our community ethos

Links to legislation and guidance

This policy has been written in compliance with the following legislation and guidance:

- Education (Pupil Information) (England) Regulations 2005
- Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR)
- Data Protection Act 2018
- GDPR guidance (ICO) including Code of practice for subject access requests, personal information, lawful bases

Associated policies and further reading

This policy should be read in conjunction with the following associated policies and documents:

- Complaints Policy
- e-Safety Policy
- Health & Safety Policy
- Safeguarding & Child Protection Policy
- Whistleblowing Policy

Definitions

Personal data – Information relating to an identifiable, individual, including:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username
- Factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.

Sensitive personal data – More sensitive personal data that needs more protection, including:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics/biometrics
- Health – physical or mental
- Sex life or sexual orientation

Processing – Processes done automatically or manually to personal data, (e.g. collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying).

Data subject – Identifiable individual whose personal data is processed.

Data controller – Person or organisation that determines the purposes and the means of processing of personal data.

Data processor – 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 – Security breach causing accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data.

Roles and Responsibilities

Directors

Directors ensure compliance with data protection legislation and regulations. It is their responsibility to:

- Represent the NEST as a data controller
- Ensure compliance with data protection legislation by appointing Data Protection Officer (see below) and ensure they are sufficiently trained and resourced to complete their duties
- Take overall responsibility for compliance
- Ensure the NEST is registered with the ICO as a data controller

Data Protection Officer (DPO)

The Data Protection Officer is responsible for implementation of this policy and monitoring compliance. It is their responsibility to:

- Develop related policies and guidelines
- Provide an annual data protection report
- Advise on data protection issues
- Be first point of contact for all data subjects and ICO
- Ensure privacy notices are accessible to those expected to consent
- Integrate privacy considerations into all policies and procedures
- Review policies, timelines, processes relating to data protection

Staff

Staff collect, store and process personal data. It is their responsibility to:

- Apply the level of care required for security and validity of personal data
- Collect, store and process personal data within the policy
- Informing the NEST of changes to their personal data
- Contacting the DPO if they have:
    - Questions about this policy, data protection law, keeping personal data secure, retaining personal data
    - Concerns with the execution of this policy
    - Uncertainty of lawful basis to use personal data in a particular way
    - Need to capture consent, draft a privacy notice, deal with data protection rights or transfer personal data outside of the EEA
    - Become aware of a data breach
    - New activities which may affect the privacy rights of individuals
    - Need for help with contracts or sharing data with third parties
- Support learners' understanding of data usage consent all contexts

Learners

Mostly learners are data subjects, but they have responsibility to:

- Ensure they understand what they are consenting to in the use of personal data, asking for assistance where necessary
- Exercise caution sharing personal information with the NEST and online
- Not intentionally attempt to violate or access the personal information of any other member of the NEST community

Caregivers

Mostly caregivers are data subjects, but they do have responsibility to:

- Inform of changes to personal data (e.g. contact details, name, address)
- Ensure they understand their consent on the basis of their own or their learner's (under 13) personal data, asking for assistance where necessary

Community voice

We value lived experience at the NEST, and we believe that centring the voice of lived experience is a route to better care. The insight of learners, caregivers, staff and collaborators are invaluable in shaping an environment of trust, collaboration and co-ownership. Intentionally prioritising the perspective of learners and caregivers supports educator understanding of learner needs and can empower learners to contribute to meaningful decision making and to take an active role in their learning. Valuing staff and collaborator feedback can facilitate closer co-working and productive communication.

We actively seek feedback and engagement around data protection from the general community but specifically those who experience data breaches.

Processes

See Safeguarding & Child Protection and Health & Safety Policies for information recorded relating to Safeguarding and Health and Safety.

Record keeping

We keep a Processing Activities Log (Appendix A) that will include: type of data, data subject, how and why we have it and store it, third party recipients, retention and security measures in place for that data.

Collecting and storing personal data

Lawful basis

We only process personal data where we have one of 6 “lawful bases” or legal reasons to under data protection law. The more commonly used at the NEST are:

- Data needs to be process so we can comply with our legal obligations – reporting employee earnings to HMRC
- Data needs to be processed to protect someone’s life – in an emergency
- The individual (or their caregiver if appropriate) has freely given clear consent – we aim for this always to be the case even when another lawful basis applies

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

Fairness and transparency

Beyond our legal obligations we feel an ethical imperative to make personal data as available to data subjects as possible whether that data is collected direct from them or from other sources.

All efforts are made to make data notices (see Appendix B for template) accessible to the data subject before they give consent. All data subjects are given DPO contact details to ensure they can maintain control over their data.

Purpose

Within data notices and logs the specific, legitimate and explicit purpose for which the data will be processed is mentioned and explained where necessary. Data collected under one purpose can only be used for that purpose.

If we later have another reason to process data, data subjects will be informed and ask for consent for further processing. Data processing must be limited to what is necessary to complete our work (e.g. recording a learner’s emergency contact details or staff training logs).

When data is no longer necessary it must be deleted or anonymised (for data analysis for quality review purposes) (see below).

Consent

In all practices the NEST seeks informed and eager consent (while able to do so, without pressure). “Consent” gained through coercion or misleading information is not valid. This will be evidenced as the completion of online consent forms to record and a verbal check to confirm understanding and

validity of consent. Ideally consent will be sought for those over 13 by both caregivers and learners. Where a learner is deemed to not be able to fully understand the implications of their consent (see Safeguarding and Child Protection Policy) the caregiver consent will be sufficient. See below for photo and video consents

For special category data written consent is required unless alternative legitimate basis exists.

Accuracy

All personal data held must be accurate and up-to-date as is reasonably possible. Reported errors are corrected (e.g. amended or erased) immediately (within 5 working days). Data subjects have an obligation to inform data controllers of changes to personal data. Data subjects can contact the DPO or complete an information update form (Appendix C) to notify of changes. When we are informed of changes to personal data, we will inform any third party organisations processing data for us of the change. This is particularly important where this information may be used to inform decisions about the individual. The DPO uses personal data log (Appendix A) to update or delete (if correction not possible) data if it cannot be reasonably assumed to be accurate.

Storage

To protect personal data from unauthorised and unlawful access, alteration, processing or disclosure, and accidental or unlawful loss, destruction or damage we adhere to the following guidelines:

- Paper records are kept locked when not in use and not displayed
- Where paper is not essential, paper records are scanned and shredded
- Digital records are kept under strong password (see e-safety Policy) – recommended to change regularly
- Install encryption software on portable devices and removable media
- Personal information stored on personal devices must also be secured (see e-safety Policy)
- Since administration is predominantly conducted through homeworking, secure private network used

Retention lengths

Personal data is kept for the shortest possible time. For learner records, that is the extent of their time with us. We will delete this information when it has been successfully transferred on to another educational establishment or the learner themselves. Annually the DPO will review the data being held, the purpose, the likely accuracy and delete anything they deem unnecessary. This may include

gaining renewed or additional consents. Anonymised data for statistical analysis may be kept longer as long as the data subject is not identifiable.

Sharing personal data

We will not normally share personal data, but the following exceptions apply:

- If the safety of staff is threatened by a learner/caregiver
- To liaise with other agencies (consent to share will be sought)
- Suppliers/contractors need data to provide a service (e.g. email service)
    - Suppliers must show they follow data protection practices
    - Data sharing agreement in place
    - Only data required for service needs shared
- Law enforcement or government bodies where there is legal obligation to:
    - Prevent or detect crime (including fraud)
    - Apprehend or prosecute offenders
    - Enforce taxation
    - Support legal proceedings
    - Safeguard learners (see Safeguarding & Child Protection Policy)
    - Participate in research – where anonymised and consent given
    - Support emergency services or local authorities responding to an emergency affecting learners or staff

If we need to transfer personal data outside the European Economic Area then it will be done within the relevant laws and cannot be done unless at least one safeguard is in place or an exemption (see Appendix D).

Pseudonymisation and anonymisation

Where possible data will be stored in a pseudonymised way where additional knowledge and access to multiple pieces of data would be required to identify the individual. Any data that are shared that do not need identifying information or for research is anonymised. All archive data is anonymised.

Disposal of Records

Personal data that is no longer needed for its original purpose is disposed of securely (including inaccurate or out of date if not able to be amended).

Secure disposal includes:

- Paper-based records shredded or incinerated
- Electronic files overwritten and deleted

Subject Access requests

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

- Confirmation their personal data is being processed
- Access to a copy of the data
- Purposes of the processing
- Categories of data held
- Who has the data and who can it be shared with
- Retention lengths/guidance on retention criteria
- Source of data (if not themselves)
- Whether automated decision-making is applied to their data (significance and consequences for them)

Subject access requests may be submitted verbally or in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Contact details (correspondence address, number, email address)
- Details of information requested

Staff receiving subject access requests must immediately forward to the DPO. All requests must be logged in the Subject Access Request Log (Appendix E)

Children

Children have ownership of their data (not their caregivers). For caregivers to make a subject access request for their child they must have the child's consent or the child must be unable to understand their rights. Children 13+ are generally considered mature enough to understand their rights. This is not always true so their ability to understand their rights will be judged on a case-by-case basis (see Medication and Safeguarding & Child Protection Policies).

Response

We may:

- Ask individual to provide 2 proofs of ID
- Contact the individual by phone to confirm their request

We will:

- Respond without delay (max 1 month of receipt). In complex cases this may be extended by 2 months (individual will be informed of the extended timeline and why it is necessary within the original 1 month)
- Not charge for the information

We will not disclose if:

- Might cause serious harm to physical or mental health of learner or other individual
- Reveal child is at risk of abuse if that would not be in child's best interest (see Safeguarding & Child Protection Policy)
- Adoption or parental order records
- Given to court concerning child

Excessive or unfounded requests

We may refuse if a request is repetitive or for the same information. We will inform the subject and inform them they have the right to complain to the ICO.

Other rights of data subjects

We also recognise and support the rights of data subjects to:

- Withdraw their consent
- Ask to rectify, erase or restrict processing of their PD or object in specific circumstances
- Challenge processing on reasons of "public interest"
- Prevent processing likely to cause damage or distress
- Be notified of a data breach if it crosses the harm threshold
- Make a complaint to ICO
- Have their data deleted ("Right to be forgotten")
- Request for personal data transfer to third party in a structured machine-readable format in relevant circumstances
- Prevent their personal data being used for direct marketing
- Object to automated decisions
- Request copy of agreements for outside EEA transfer

Requests for any of the above submitted to DPO. If staff receive, they forward it

Educational records

Caregivers have a legal right to their child's educational record within 15 working days of a written request.

Images and likenesses

CCTV

We do not use CCTV at the NEST but the Dee Space Community Centre does have CCTV on the entrance. The use of this is managed through their Data Protection and CCTV policies which we have read.

Photographs and videos

There are legitimate reasons that we may take photos and videos of learners and staff. As part of admission, caregivers are asked for their consent for photos of their young people to be taken, stored and used for educational purposes only or also for marketing/promotion purposes. Learners 13 and over and also asked for their consent for their photo to be used both formally (Appendix F) and verbally each time before a photo is taken and once it has been taken their consent is confirmed. Consent can be withdrawn or refused at any time. Where consent is withdrawn the photo or video is deleted from any place it is stored locally or online including the website or social media. All photos and videos are stored under encryption.

Where photos and videos are used for assessment purposes they may be seen at presentation days to caregivers. Learners told about who is able to see it and asked for consent for their image being used in presentations. Where relevant they can choose not to present or to add obscuring details to images.

If a photo or video is selected to potentially be used for promotional purposes the caregiver and learner are given the opportunity to object and edit as part of their right to consent. The use of the media will be clearly explained as part of this additional consent. Where photos or videos are used the faces of learners must be obscured and no additional information such as name or age will be included to minimise identification.

Personal data breaches

We try to at all costs prevent personal data breaches. If it does happen then we follow the personal data breach protocol (Appendix G). The DPO is the contact person for all stakeholders including the ICO. Certain breaches (see Appendix G) must be reported to the ICO within 72 hours. For these, the DPO must complete an assessment of the breach in these 72 hours. If necessary, the DPO informs any affected data subjects. Contracted data processors must inform the NEST DPO of any breach within 72 hours.

We recognise data subjects' right to compensation if they have suffered material or nonmaterial damage as an infringement of data protection legislation. Claims will be dealt with through complaints procedure (see Complaints Policy).

Examples of data breaches

- A non-anonymised dataset being published on the provision website
- Safeguarding information made available to an unauthorised person
- Theft of a provision laptop containing non-encrypted personal data

Impact assessments

When the processing of personal data by the NEST or another organisation on our behalf is using new technologies, or where it presents a high risk to the rights and freedoms of data subjects, a Data Protection Impact Assessment (DPIA: Appendix H) is completed before processing. A single DPIA may assess a similar set of processing operations with similar risks.

Where a DPIA finds that the proposed processing could cause damage and/or distress to data subjects or otherwise high risk, the processing will not commence and Directors and DPO must review. If necessary, the DPO will escalate concerns to the ICO.

Training

Staff training, learning and development are highly encouraged and facilitated by the NEST. All staff are expected to complete minimum training requirements as outlined in our Staff Training Plan and additional learning and related continued professional development are strongly supported.

All staff are introduced to this policy. Directors, including the Data Protection Officer will complete GDPR training.

Review

This policy will be reviewed annually at a minimum. Updated policies will be made available locally and on our website (www.thenest-ed.uk). Ad hoc amendments will be made as new information becomes available and to align with any legislative changes as they arise. Stakeholder feedback, particularly that of learners and caregivers, will be invited and incorporated as much as is practicable. Where quantitative data are available these will be analysed and embedded in policies updates.

Data relating to data breaches, data security audits and DPIAs will be analysed to identify areas for improvement in the processes. The DPO conducts an annual audit (ICO audit toolkit) of privacy measures and their effectiveness to conform to current law and guidance. The DPO will present an annual report monitoring and reviewing the application of this policy.

Appendices

Appendix A – Processing Activities Log

Appendix B – Privacy notice template

Appendix C – Update form for personal data

Appendix D – Safeguards and exemptions for data transfer outside the EEA

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

- Adequacy decision
- Privacy shield
- Binding corporate rules
- Model contract clauses

In the absence of the above, a transfer of personal data to a country outside the EEA or international organisation shall only take place if:

- Data subject has explicitly consented (after being informed of possible risks) to the proposed transfer without adequacy decision and appropriate safeguards
- Transfer is necessary for:
    - performance of a contract between data subject and data controller (including pre-contractual measures at the subject's request).
    - performance of a contract in the interest of the data subject between the data controller and another natural or legal person
    - important reasons of public interest
    - establishment, exercise or defence of legal claims
    - protect vital interest of the data subject or other persons where the data subject is incapable to give consent

Appendix E – Subject Access Requests Log

Appendix F – Learner consent for photography

Appendix G – Personal Data Breach protocol

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach or potential breach, staff or data processor immediately notifies DPO
- DPO investigate and determine if a breach has occurred. Has personal data been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed where it should not have been
    - Made available to unauthorised people
- DPO will alert Directors
- DPO make every effort to contain and minimise the breach (assisted by staff or processors as necessary) – specific actions for data types set out at the end of this procedure
- Will assess potential consequences – how serious x likelihood
- Does the breach need to be reported? Case by case. the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, Material or non-Material damage (e.g. emotional distress), including through:
    - Loss of control of their data
    - Discrimination
    - Identity theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation
    - Damage to reputation
    - Loss of confidentiality
    - Other economic or social disadvantage to data subjects

  If it is likely risk to rights and freedoms DPO must notify ICO

- DPO will document decision (Additional appendix?) to provide paper trail digitally.
- Where ICO must be notified, "report a breach" page ICO website within 72 hours including:
    - Description of the nature of the breach:
        - Categories and approximate number of individuals concerned
        - Categories and approximate number of personal data records concerned
    - Name and contact details for DPO
    - Likely consequences
    - Measures taken and planned to mitigate

If the details are not yet known they will report what they can in 72 hours, report should explain the delay and reasons and expectations of when to have the full report. Submitted ASAP

- Reassess risk to data subjects – if risk is high will write to all data subjects including:
    - Name and contact details for DPO
    - Likely consequences of the breach
    - Measures that have been taken/planned to mitigate
- DPO inform relevant third parties who can minimise loss for individuals
- Document each breach on encrypted shared drive even if not reported to ICO including:
    - Facts and cause
    - Effects
    - Action taken (containment and improving processes)
- DPO and Directors meet to review and prevent it happening again as soon as reasonably possible
    - Consider disciplinary action for staff if relevant

Appendix H – Data Protection Impact Assessment template