Data Protection and Information Security Policy

26 Aug 2026, 48 min read

> **Operated by:** Nudge Education Ltd · **Version:** Dec 2025 · **Owner:** Data Protection Officer

Nudge Education Data Protection & Information Security Policy

December 2025

Review Date; December 2026

Scope of Document;

This policy is drafted to ensure that all personal data relating to our students, staff, associates and clients is kept and processed in a manner that keeps Nudge Education compliant with The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025 (together, "data protection laws").

This policy is linked to several other key documents such as our Safeguarding & Child Protection Policy, Confidentiality Policy,Privacy Policy, Social Media Policy & IT Policy as well as our Business Continuity Plan Statement of Intent

Nudge Education supports some of the most vulnerable students in the United Kingdom to transition back into a permanent setting of education, further training or employment and as such, we appreciate that the protection of their human rights is vitally important in engaging them. Many of these students may present risk behaviours, have legal conditions surrounding them and their family members and may be placed in a secure location where it is essential that staff, associates and agents of Nudge Education stringently follow the principles of UK GDPR which are that data;

1. Be processed fairly and lawfully

2. Be obtained only for specific, lawful purposes

3. Be adequate, relevant and not excessive

4. Be accurate and kept up to date

5. Not be held for any longer than necessary

6. Processed in accordance with the rights of data subjects

7. Be protected in appropriate ways

8. Not be transferred outside the European Economic Area (EEA), unless

that country or territory also ensures an adequate level of protection

Nudge Education agrees to adhere to the above to ensure high levels of data security and protection to safeguard an individual's right to data protection.

Although the focus of our organisation will always be the students that we work with, we also implement this policy to ensure that the personal data of our staff, associates and clients are also protected.

The following sources and documents have been used to inform our policy.

Data Protection Act 2018

www.cyberessentials.ncsc.gov.uk/advice/

Guide to the General Data Protection Regulation (ICO 2018)

The Data Protection Officer for Nudge Education is: The Data Protection Lead, 07958 440937 (business mobile).

The Children's Commissioner at the time of this policy is: Dame Rachel de Souza and she; "speaks up for children and young people so that policymakers and the people who have an impact on their lives take their views and interests into account when making decisions about them."

(**https://www.childrenscommissioner.gov.uk/about-us/the-childrens-commissio** ner-for-england)

Nudge Education Data Protection and Information Security Policy Dec 25
To contact the Children's Commissioner you should call 020 7783 8330 or go to: **https://www.childrenscommissioner.gov.uk/about-us/contact/** for more information.

Ofsted is the Office for Standards in Education, Children's Services and Skills. We inspect and regulate services that care for children and young people, and services providing education and skills for learners of all ages. To get in touch with Ofsted go to **www.ofsted.gov.uk** for further information.

Data Protection Policy Scope of this policy

This policy applies to all personal and special category personal data processed by Nudge Education in any format and whether processed by us in the role of data controller or a data processor.

This policy is applicable to all Nudge Education trustees, employees (permanent and temporary), volunteers, partners, and third parties who have access to the personal data Nudge Education processes, or to Nudge Education's systems which process personal data.

Roles and responsibilities

All staff have responsibilities in relation to this policy and certain roles have additional responsibility, as follows:

1.1 Chief Executive Officer

The Chief Executive is the accountable officer responsible for the management of the organisation and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and thus maintaining confidentiality is pivotal to the organisation being able to operate.

1.2 Data Protection Officer & Information Security Manager

The Data Protection Officer is responsible for monitoring and ensuring compliance with this policy and overseeing the lawful processing of all personal and special category data processed by Nudge Education.

It is the Data Protection Officer's responsibility to fulfil the tasks of a Data Protection Officer as set out in UK GDPR Article 39, that is:

- to inform and advise Nudge Education and its employees of their data protection responsibilities as a controller and processor of personal data
- to monitor compliance with data protection legislation and this policy
- to provide advice where requested on Data Protection Impact Assessments (DPIAs)
- to co-operate with and act as the contact point for the ICO (UK's supervisory authority) Nudge Education Data Protection and Information Security Policy Dec 25
- to be the contact point for data subjects with regard to all issues related to the processing of his or her data

The Data Protection Officer is also responsible for seeking guidance from the Head of Information Security where data security concerns arise and shall provide advice and guidance to the organisation regarding the lawful and appropriate processing of personal and special category data.

Information Security Manager

The Head of Information Security shall provide technical support and guidance around the secure and confidential processing of personal and special category data within the organisation and shall be responsible for addressing any data security concerns.

The Head of Information Security is responsible for the organisation's Information Security Management Policy and for reporting relevant information to senior management.

The Head of Information Security will ensure that any information security incidents are appropriately managed and will support the Data Protection Officer with information security matters as required.

Both roles, Data Protection Officer and Information Security Officer, lie with the Data Protection Lead, Director of Operations, 07958 440937.

1.3 Process owners

Data processing activities are managed by nominated job roles or individuals. Senior Management shall ensure that a process owner is assigned to each data

processing activity or operation. The Process Owner has primary operational responsibility for compliance with data protection legislation and good practice in respect of assigned processing activities.

Process Owners are responsible for understanding what personal data are used in their business area and how it is used, who has access to it and why. As a result, they are able to understand and address risks to the data and the organisation. Where the nature of the organisation's activities is such that personal data are processed as part of a single business process across a number of separate hierarchical business units then, responsibility for the business process as a whole may be assigned to one named Process Owner.

The Data Protection Officer shall maintain a list of Process Owners and the data processing activities they are responsible for. Process Owners may delegate day-to-day responsibility for compliance within their management hierarchies, subject to other HR policies and ensuring that all staff are appropriately trained.

Nudge Education Data Protection and Information Security Policy Dec 25

1.4 Employees, volunteers, casual/temporary workers, directors and officers

etc. Anyone who is directly engaged by the organisation, including but not limited to employees, volunteers, casual/temporary workers, directors and officers etc. must adhere to this policy and all associated procedures. Employees must only process personal data as authorised and necessary for the completion of their duties. All processing must be carried out in accordance with data protection legislation and this policy and associated procedures. Employees must never process personal data of identifiable individuals unless the processing is part of their work or they have been specifically authorised by the Data Protection Officer to do so.

Employees shall report any actual or suspected non-compliance or concerns regarding the processing of personal and special category data to the Data Protection Officer without delay.

Employees must attend data protection and data security training as required.

Employees must report all actual and suspected personal data breaches in accordance with our Personal Data Breach Procedure.

Everyone within the Organisation has a duty to respect data subjects' rights to confidentiality.

Disciplinary action and / or penalties could be imposed on staff for non-compliance with relevant policies and legislation.

Policy Detail

1.5 Special category data / criminal conviction and offence data

Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The organisation shall not process special categories of personal data unless it is necessary. Where the processing of special categories of personal data is necessary, the Data Protection Officer shall ensure that the lawful grounds for such processing are documented and shall maintain a periodic review of the necessity to processing the special categories of personal data.

If the organisation is processing personal data relating to criminal convictions and offences it shall implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

1.6 Principles

The organisation will ensure any processing of personal data is carried out in compliance with Data Protection Principles as detailed below.

Fairness - The organisation shall ensure personal data is processed fairly and in compliance with legislation at all times. Nudge Education Data Protection and Information Security Policy Dec 25 Lawfulness - The organisation will ensure there is an applicable lawful basis to facilitate all processing of personal data and special category data. Where the lawful grounds are legitimate interests a legitimate interests assessment (LIA) will be undertaken and documented. Where the lawful grounds are a task carried out in the public interest or in the exercise of official authority vested in the organisation, a public interests

assessment (PIA) will be undertaken and documented. Where the lawful grounds are a legal obligation, the relevant legislation shall be cited and appropriately documented. Where the lawful basis is consent or explicit consent the organisation shall ensure the consent is valid and that the data subject is able to withdraw their consent should they choose to.

Consent shall not be valid unless:

- there is a genuine choice of whether or not to consent;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;
- the organisation can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully; and
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent.

The organisation recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. The organisation recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing. Where consent is the lawful basis for processing, the Data Protection Officer shall ensure that consent is properly obtained in accordance with the conditions above.

Transparency - The organisation shall ensure that transparency is engrained in the processing undertaken. Before any processing of personal data begins, the privacy information provided to data subjects will be considered and will be updated where necessary to ensure it accurately reflects the processing being undertaken.

Purpose Limitation – The organisation shall ensure personal data is collected for specified, explicit and legitimate purposes and not further processed in a

manner that is incompatible with those purposes.

Data Minimisation – The organisation shall ensure personal data is adequate, relevant Nudge Education Data Protection and Information Security Policy Dec 25 and limited to what is necessary in relation to the purposes for which they are processed. The organisation will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collects.

Accuracy - The organisation will use its reasonable endeavours to maintain data as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date.

Storage Limitation - The organisation will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymization.

Security - The organisation will ensure that any personal data that it processes or commissions the processing of is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In particular, an information security management policy (ISMP) will be maintained setting out specific policies in relation to ensuring the confidentiality, availability and integrity of personal data.

Accountability - The Data Controller is responsible for, and must be able to demonstrate compliance. This means that the organisation must demonstrate that the six principles outlined above are met for all Personal Data for which it is responsible. The management will implement sufficient controls to ensure that it is able to demonstrate compliance with the Data Protection Legislation including the keeping of sufficient records of data processing activities, risk assessments and relevant decisions relating to data processing activities.

1.8. Individual Rights under Data Protection Legislation and Freedom of Information The organisation will ensure that all personal data processing respects the rights and freedoms of individuals, and that appropriate policies and procedures are in place to effectively manage any requests received in relation to these rights.

The organisation shall take appropriate steps to advise individuals of their rights and ensure that employees are able to recognise and appropriately handle information rights requests, including those made under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Freedom of Information Act 2000 (FOIA).

Rights under the UK GDPR and DPA 2018 Individuals have the following rights in relation to their personal data:

- Right to be informed about the collection and use of their personal data
- Right of access to personal data (Subject Access Request)
- Right to rectification of inaccurate or incomplete personal data
- Right to erasure of personal data ("the right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object to processing (including direct marketing)
- Right not to be subject to decisions based solely on automated processing, including profiling Nudge Education Data Protection and Information Security Policy Dec 25
- Right to lodge a complaint with the Information Commissioner's Office (ICO) and to seek a judicial remedy and compensation where applicable

The Data Protection Officer (DPO) shall maintain a procedure outlining how personal data rights requests are to be handled and ensure that all relevant staff are aware of it. Rights under the Freedom of Information Act 2000 (FOIA).

As a public authority, the organisation is also subject to the Freedom of Information Act

2000. This provides members of the public with a general right of access to recorded

information held by the school, regardless of whether it contains personal data.

Requests under FOIA will be handled in accordance with the statutory requirements, including the duty to:

- Confirm or deny whether the information is held; and
- Communicate that information, unless an exemption applies.

The school will ensure that staff understand the distinction between personal data requests (handled under UK GDPR/DPA 2018) and general information requests (handled under FOIA 2000), and that both are managed in line with established procedures and statutory timeframes.

1.1 Personal Data Breaches

The organisation will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this personal data breaches policy. All employees and individuals with access to personal data for which the organisation is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach (whether this is actual or suspected). The organisation will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The Personal Data Breach Procedure sets out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach. The Data Protection Officer shall be responsible for maintaining the Data Breach Reporting Procedure and for ensuring that all relevant people are made aware of it.

1.2 Data Sharing and Data Processors

The organisation will only share personal data where we have a lawful basis and it is necessary to do so. Where we share data with third parties / processors we shall carry out appropriate due diligence and ensure there is an adequate Data Sharing Agreement/Data Processing Agreement in place prior to any sharing of personal data with third parties.

The Data Protection Officer shall maintain a record of all with whom data is shared and all data processors, and is responsible for ensuring that appropriate agreements are in place. Nudge Education Data Protection and Information Security Policy Dec 25 The Data Protection Officer shall be responsible for maintaining the Data Sharing Procedure and the Selecting, Appointing,

Managing and Decommissioning Data Processors Procedure and for ensuring that all relevant people are made aware of them.

1.3 Restricted Transfers

The organisation will only transfer data outside of the UK where it is strictly necessary to do so. Prior to transferring any personal data outside of the UK (referred to as a restricted transfer) the organisation will take steps to ensure there are appropriate data transfer mechanisms in place to safeguard the data. The Data Protection Officer shall be responsible for maintaining the Restricted Transfer Procedure and for ensuring that all relevant people are made aware of it.

1.4 Children's data

Special measures will be taken by the organisation if it processes personal data relating to children under the age of 13 including the nature of privacy information provided and approach to information rights requests. These special measures will be set out in a policy relating to children's data.

1.5 Data Protection Impact Assessments (DPIAs)

The organisation will adopt a risk-based approach to processing personal data ensuring that it assesses any risks to privacy or to the rights and freedoms of people before commencing, commissioning or changing data processing activities. Where necessary it shall, as a minimum, ensure that a DPIA is undertaken where required by Data Protection Legislation and/or when one is deemed to be desirable by the Data Protection Officer.

The Data Protection Officer shall be responsible for maintaining the Undertaking DPIA's Procedure and for ensuring that all relevant people are made aware of it.

1.6 Electronic marketing

The Organisation is subject to certain obligations under PECR when performing marketing activities to customers. It shall ensure that appropriate consents are recorded prior to the sending of marketing materials unless the "soft opt in" applied.

The limited exception for existing customers, known as “soft opt in”, allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The organisation shall explicitly offer the right to object to direct marketing to the data subject at all stages of communication and in an intelligible manner so that it is clearly distinguishable from other information. A data subject’s objection to direct marketing shall be promptly honoured. If a data subject opts out at any time, their details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

1.7 Privacy by design and by default

The organisation shall consider privacy by design and by default when processing Nudge Education Data Protection and Information Security Policy Dec 25 personal and special category data. Privacy by design and by default is a legal obligation. Privacy by design and by default requires organisations to consider data protection issues at the design stage of the processing and throughout its cycle.

1.8 Training and awareness

The organisation will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically.

Document Control The Data Protection Officer owns this procedure and is responsible for ensuring that it is reviewed on a regular basis. A current version of this procedure is available to all employees on Nudge Education’s Intranet.

This procedure was approved by the Director or Operations on 5th December 2025 and is issued on a version-controlled basis under his signature.

Signature: Date:

1.7Change History Record

Version Date Details of Change(s) Approved By 2.0 5/12/2025 Implementation of V2 policy Director of Operations

PAGE IS INTENTIONALLY BLANK

Nudge Education Data Protection and Information Security Policy Dec 25 Information Security Policy Human Resources Security Policy

In line with our Recruitment & Selection Policy, Nudge Education carry out the following checks on all our staff and associates/contractors prior to them commencing work for us;

- Produce valid documentation proving their identity including photo identification
- Provide evidence showing they have the right to work in the UK: (Passport, Birth Certificate and other documents listed at; **https://www.gov.uk/legal-right-work-uk**)
- Provide a full employment history accounting for any gaps; and
- Undertake an enhanced Disclosure and Barring Scheme (DBS) check (or provide evidence of their update service status). This must be renewed every three years if not on the update service.
- Supply three recent and valid references (2 must be professional or academic)
- Provide evidence of relevant training and qualifications (originals only, copies will not be accepted)
- All staff and associates who apply to work with Nudge Education will be processed via the Department for Education's Employer Access service (**https://www.gov.uk/guidance/check-a-teachers-record**)This is whether they disclose they are a qualified teacher or not to ensure that anyone providing us with false or inaccurate information is identified.
- Check to see if they have any other positions of trust held in other organisations (e.g. Governor, Sports Coach etc.)

Staff and contractors will be given a full induction on Data Security and Protection. This is provided via a range of methods from online learning to a practical 1:1 instruction

Regular updates on data security and protection matters are emailed out and communicated directly during conversations and reviews of performance.

It is also a requirement for all staff and associates to maintain their knowledge of data protection which must be evidenced on their staff/associate record.

Any failure to comply with this policy will be investigated and relevant disciplinary action taken, or in the case of contractors, activation of a termination clause in their contract.

We maintain all staff and associate data for a period of seven years in a secure cloud-based archive until it is destroyed/deleted.

Nudge Education Data Protection and Information Security Policy Dec 25 Asset Management Policy

Nudge Education owns a number of devices such as phones and laptops that have the capacity to store data. For this equipment the organisation will ensure that;

- Devices are password protected
- 2-Step verification is enabled in the case of theft or misplacement of equipment (**https://www.google.com/landing/2step/**)
- Devices that are de-commissioned will be wiped of all sensitive data using appropriate software or using a trained and vetted professional to carry out this function.
- To destroy assets securely that are owned by Nudge Education, we will use a service to crush or shred devices & hard drives
- Where it is identified that a device could be recycled, in line with our environmental policy, an appropriate service should be used (**https://www.recycleyourelectricals.org.uk/how-to-recycle-electronics/**)

Devices that are owned by associates or contractors are out of scope for this policy but we do require all associates to have a specific email account whilst working with us that is separate from their personal account and that they will comply with our own data protection policies and protocols.

All staff and associates that use their own devices will be subject to our separate use of own devices policy which contains the following stipulations:

- All devices used for work with Nudge Education must have a separate profile/login from their personal profile.
- Sensitive data should only be downloaded when absolutely necessary and deleted from the local device as soon as it is no longer needed
- It must follow the same password protocol as devices owned by Nudge Education
- Any breaches of data must be reported in the same was as per the data breach reporting process

Decommission and disposal of Information Assets

All information assets will be destroyed when they reach the end of their useful life. This includes the decommissioning of servers, network devices and any data storage devices. All such destruction is appropriately certified and logged against the IT Asset Register. System Architect is responsible for all IT Assets throughout its useful life and for complying with the decommissioning processes. The current System Architect at Nudge Education: 07961 226726 (business mobile)

Physical Environment Security Policy

Nudge Education will ensure that in properties that it operates, owns or leases it will;

- Provide access to only those authorised to be there
- Keep a log of keyholders for those premises
- Operate a clear desk policy to ensure that no sensitive information is

Nudge Education Data Protection and Information Security Policy Dec 25
left unattended.

- This will also apply to printers and scanners.
- Lock away sensitive data when not being used.
- Destroy any data that is no longer needed using a shredder that is at least to DIN level 4 (for Highly Sensitive Data)
- Ensure that any whiteboards or notice boards do not contain any sensitive data that can be linked to anyone.
- All visitors will be required to sign in and out of the premises in a written log.

In properties that Nudge Education uses for education it will;

- Assess venue for considerations of privacy and security
- Remove any sensitive data at the end of the session
- Ensure that any IT equipment owned by the company has appropriate security measures such as password protection and content controls are implemented
- Ensure that IT equipment owned by associates or contractors have similar levels of security by carrying out regular checks.
- Monitor online safety of students when they are using IT equipment to ensure they are safeguarded against risks of grooming, identity theft and other associated issues.

Protection against Malicious and Mobile Code

The organisation uses a variety of incident detection and prevention tools as well as web scanning protection as a core element of our security controls. This is designed to protect from a wide range of threats to confidential information, unauthorised re-direction to inappropriate web locations, and loss of network performance.

It employs the latest scanning engines to deliver protection from the most sophisticated and targeted web-based threats, including spyware, Trojans or other malware. It ensures that web requests (including The web pages, images and larger files such as PDFs, or media) are free from malicious code before they reach our employees. The service also includes the latest URL filtering and DDOS protection and blocking functionality. The organisation has installed anti-virus software on all corporate PCs and laptops. Virus signatures are kept up to date by an automated process which pushes updates to end-user devices as these become available. In addition to this, we scan our internal networks to ensure that viruses and malware have not been able to enter by any other means. Regular vulnerability scanning is used to detect weaknesses in externally facing IP addresses.

The organisation has a process for monitoring logs of internally averted viruses and investigating the source of the vulnerability, to verify that acceptable usage policy is being followed.

System Back-up

Nudge Education backup cycles are four-weekly, with Google Take-Out being used to export data from our Google Drive. Staff are required to regularly

back-up their data using this service. Nudge Education Data Protection and Information Security Policy Dec 25 Centrally created data is backed-up and securely stored off-site using a different provider from our main server hosting. The backup files are encrypted with AES256 using opens and are transmitted over SSL.

The System Architect is responsible for ensuring a robust backup and recovery process that minimises the risks and operational impact to the organisation and its clients from service interruptions and potential loss of data integrity.

All client data held on the organisation’s servers and storage devices are backed up to an offsite data centre. All offsite locations are visited to ensure that the location is physically and environmentally secure.

Network Security Management Within Nudge Education internal business environment, a range of network controls are in place to achieve and maintain security; some details on network security measures are considered restricted and so not listed externally. The following controls form part of those measures:

- L3/L4 security firewalls around infrastructure platforms
- Google Admin provides user authentication onto the network for access to general office applications (Docs, Sheets, Gmail etc). System policies are set to enforce password complexity and change intervals. Only “strong” passwords are allowed, and rules are set to prevent re-use of existing passwords
- Further user authentication such as Passkeys or 2-Step authentication is required to access systems. Role based access rights are implemented to enforce segregation of duties and financial approval levels
- Physical and logical segregation exists between Nudge Education internal business network and the networks Nudge Education uses to provide service to clients
- The internal WiFi network is WPA2 with password protection

Incident Reporting & Management The organisation has procedures in place for reporting, investigating and managing security and operational events and incidents. Refer to the Breach Reporting Procedure for guidance.

Cyber-security threats Always exercise caution when receiving any unexpected e-mails, particularly from an unknown source; if in doubt, users should always

consult the System Architect for advice and guidance.

Immediately report any suspicious activity or suspected breach in security, including the loss or theft of any information asset, to the System Architect and/or the Data Protection Officer in accordance with the Personal Data Breach Procedure.

Password Policy Nudge Education Data Protection and Information Security Policy Dec 25 User-IDs and associated passwords are designed to protect our data by restricting access to authorised personnel only. All users are responsible for any action performed under their personal user-ids that have been allocated to them. To maintain the company's system and data integrity you must adhere to the following guidance

- All Nudge Education devices and software must be authenticated by the use of User ID's and passwords.
- Minimum password length: Passwords must be at least 12 characters long.
- Complexity requirements: Passwords must include a combination of uppercase and lowercase letters, numbers, and special characters (e.g., !, @, #, $, %, ^, &, *).
- No easily guessable information: Passwords should not contain easily guessable information such as user's name, username, date of birth, or common words/phrases.
- Password history: Users cannot reuse any of their previous 5 passwords.
- Two-factor authentication (2FA): Whenever possible, enable 2FA for an additional layer of security.
- You must not write down or share your password or PIN with anyone else
- When leaving your Laptop unattended for any period of time and especially when leaving the office you must ensure that it cannot be accessed by anyone else. The following actions must be undertaken: o When leaving the office for a short period of time LOCK your Laptop (e.g. using the CTRL/ALT/DELETE keys); o When leaving the office for the day turn off your laptop and store it in a safe place at home;

Compliance We will comply with Data Protection Legislation, client specific requirements and any other relevant industry guide. We work closely with all of our clients to identify and address any specific security and any other

reasonable, legal, requirements that they may have and will be defined in an agreed contract and/or data processing agreement.

Compliance Checking and Management Review Nudge Education, supported by its retained consultants Data Protection People Ltd, formally audits its information governance and security systems on an annual basis and makes any identified corrective actions as required.

The System Architect review all reported incidents and audit recommendations and sign-off any required corrective actions. The System Architect in conjunction with the Data Protection Officer oversees the subsequent implementing of any corrective actions and reports back to the Chief Executive Officer accordingly.

Breaching the terms of this policy A deliberate breach of any of the Policies and Procedures within the framework and its related policies will be considered to be gross misconduct and/or breach of contract. It may be dealt with following the Disciplinary and Capability Procedure contained within the Staff Handbook. Serious offenders are liable to prosecution under the Computer Misuse Act 1990 and the Data Protection Act 2018 or other applicable legislation. Nudge Education Data Protection and Information Security Policy Dec 25 Confidentiality As an employee of, or contractor to, Nudge Education, you may come into contact with commercially sensitive information or personal information relating to the organisation, its staff or those of its clients.

You must not under any circumstances disclose any such information outside of the organisation without the prior approval of the System Architect.

If you are asked for information about our work (e.g. from the media) then do not attempt to deal with the query yourself but refer it to the Director of Operations If someone contacts you wanting specific information relating to one of our students, you must cross reference the caller’s information with data held on our system, ideally all requests for information must come via the nominated email that we have on record and then can be verified via phone.

Nudge Education Data Protection and Information Security Policy Dec 25 Communication & Access Security Policy

Nudge Education will strive to ensure that the organisation will use the following protocols;

- When sending calendar invites, group emails or bulk communications, a Blind Carbon Copy (BCC) message will be used to protect the recipient's privacy.
- Encryption software will be used when emailing sensitive or confidential data. As of 2025, GMail is the service that is used for email at Nudge Education. This carries Transport Layer Security (TLS) which means it is protected when being transported to most major email services
- Some commissioners may require us to use a specific email encryption service (such as Egress Protect) which we will agree to use rather than our normal Gmail Service for communications with them.
- Where an email is sent by us that needs to have an attachment containing sensitive data, this should be sent as a link to the file in our Company drive, which will have restricted access, rather than attaching to the email itself
- Where required, Confidential Mode should be used for sending sensitive information that cannot be attached with a passcode and expiry date that is appropriate for information being sent.
- Staff and associates will only refer to a student in written or electronic communication by their initials, or an Agreed pseudonym (eg. JoSm for John Smith)
- Devices will be locked with a password when not in use to protect sensitive information. A lock timer should be set for that particular device that is appropriate for the environment is it being used.
- Sensitive information will not be kept locally on a device and must be regularly uploaded to the secure company drive.
- Passwords for accounts that are used to link in to the Nudge Education Google Drive are to be changed monthly. Passwords should be at least 8 characters with upper and lower case letters, a number and special character
- Staff and associates must update software on their device on a regular basis as this will ensure that they are working with the most recent and secure version. Having outdated software increases risk of a cyber-attack.
- Access to folders on the Google Drive will only be allocated to those people who are approved, vetted and need to have the information
- Staff and associates will only be given data that they have an appropriate need for and this access will be removed as soon as they no longer require access to that data.

Nudge Education Data Protection and Information Security Policy Dec 25

- Documents that need to be shared with more than one person will be either saved in a PDF format so can't be edited or users will be given read-only access to document which can't be downloaded
- Unencrypted USB sticks are not permitted to store any data belonging to Nudge Education or its commissioners.

Business Continuity Plan (Information Security)

We have a current business continuity plan that supports this policy. Key points of this plan include

- All sensitive company data is stored on the Google Drive system which is automatically backed up.
- Data on Google Drive cannot be deleted and if documents are sabotaged there is a function to retrieve previous versions of documents easily.
- If data needs to be physically transferred to approved stakeholders, this will be sent via an encryption service such as Egress Switch, or downloaded onto a storage device that supports 256-bit encryption and sent by secure mail or delivered in person.
- Router passwords are changed from factory default password upon installation
- Routinely change passwords on all devices and accounts with 8 character alphanumeric & special characters
- There will be a limited number of people with access to administrator accounts such as the Google Admin dashboard that only has two approved users.
- Software is removed as soon as no longer needed or updated
- Laptops will be secured with single user accounts on devices owned by Nudge Education
- Outgoing staff and associates have their access removed at point of departure
- Only approved 'whitelisted' apps will be allowed to be downloaded onto devices
- Critical updates are installed within 14 days of release

Leaver Control Process

For Staff that leave employment or associates who cease contracting with Nudge Education, the following steps will be taken;

- Access to all folders on Google Drive will immediately be revoked.
- A request for any identification badges to be returned or evidence it has been destroyed will be made.
- To mitigate the risk that the ID badge will not be destroyed, Nudge Education put a six-month expiry date on each card that is given out with a phone number to call to check the ID of person who has the card.
- All IT assets will be returned to Nudge Education with monies being withheld until it has been received.
- Devices to be wiped of all data before being passed to new staff member/ associate Nudge Education Data Protection and Information Security Policy Dec 25
- Keys to office buildings and filing cabinets and equipment are to be returned with monies being withheld until they are received
- Security/reception staff to be informed of person exiting the business
- Any credit cards/petty cash/ cheque books must be returned prior to exiting the organisation.
- Any printed or hardcopy data that is owned by Nudge Education is to be returned.
- An Exit review is to be held to remind outgoing people of the need for confidentiality relating to business matters.

1.8Change History Record

Version Date Details of Change(s) Approved By 2.0 5/12/2025 Implementation of V2 policy Director of Operations

Nudge Education Data Protection and Information Security Policy Dec 25

NEO Online Addendum

This addendum applies the canonical Nudge Education policy above to the online provision context of Nudge Education Online (NEO). It is sourced from `NEO - Data Protection, Confidentiality and Privacy Policy v04.26.docx`.

NEO BY NUDGE EDUCATION

Data Protection, Confidentiality and Privacy Policy Nudge Education Online

Policy Owner	**Data Protection Officer (DPO) — function held by the Director, NEO & Head of School during the initial period, subject to review according to the growth rate of the organisation**
Approved	April 2026
Review Date	April 2027
Version	04.26
Operating Company	Nudge Education Ltd (Company Number 10192753)
Proprietor	Proprietor, Nudge Education Ltd
Accreditation Route	Online Education Accreditation Scheme (OEAS) — accreditation in progress

This policy applies to all learners, staff, practitioners, contractors, volunteers and visitors of Nudge Education Online (NEO). NEO is a fully online alternative provision for learners aged 11–18, operated by Nudge Education Ltd. NEO is not a DfE-registered independent school and is not subject to Independent Schools Inspectorate (ISI) inspection. NEO is pursuing OEAS accreditation only.

1. Statement of Intent

Nudge Education Online (NEO) is committed to respecting the privacy, dignity, and safety of all learners, staff, and families. As a fully online alternative provision serving learners aged 11–18, NEO processes personal data across digital platforms as an inherent part of delivering education, maintaining safeguarding, and meeting statutory obligations. NEO aims to: Protect the rights of individuals under the UK GDPR, the Data Protection Act 2018, and the ICO Children's Code. Embed privacy, confidentiality, and security as standard

practice across all digital operations. Share information appropriately to uphold safeguarding, wellbeing, and legal compliance. Maintain robust systems for preventing, detecting, and responding to data incidents. Ensure that all data processing is lawful, fair, transparent, and proportionate.

2. Scope

This policy applies to all staff, practitioners, contractors, volunteers, the Proprietor, and any person processing personal data on behalf of NEO. It must be read alongside the NEO Child Protection and Safeguarding Policy, Online Safety and Acceptable Use Policy, Behaviour and Regulation Policy, and SEND Policy. NEO is not a DfE-registered independent school and is not subject to ISI inspection. NEO is pursuing OEAS accreditation only. The ICO and external data protection regimes apply to NEO in the same way as they apply to any controller of personal data, irrespective of accreditation status.

3. Legal Framework

UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Freedom of Information Act 2000 Protection of Freedoms Act 2012 The Education (Pupil Information) (England) Regulations 2005 (as amended) The Privacy and Electronic Communications Regulations 2003 Online Safety Act 2023 Keeping Children Safe in Education 2026 (KCSIE) Information Sharing: Advice for Practitioners (DfE, 2018) ICO Guide to the UK GDPR ICO Children's Code (Age Appropriate Design Code) OEAS accreditation criteria (data and information governance strand)

4. Data Protection Principles

NEO processes personal data to support learning, meet statutory duties, manage operations, and maintain safeguarding. All processing adheres to the six principles of the UK GDPR: Lawfulness, fairness, and transparency — personal data is processed lawfully, fairly, and in a transparent manner. Purpose limitation — data is collected for specified, explicit, and legitimate purposes. Data minimisation — data collected is adequate, relevant, and limited to what is necessary. Accuracy — personal data is accurate and, where necessary, kept up to date. Storage limitation — data is kept in a form that permits identification for no longer than necessary. Integrity and confidentiality

— data is processed in a manner that ensures appropriate security. The seventh principle of accountability applies across all of the above: NEO must be able to demonstrate compliance.

5. Types of Personal Data Processed

5.1 Learner Data

Name, date of birth, address, and contact details SEND information, EHCP documentation, and health or medical needs Attendance, engagement, and academic progress records Safeguarding records and referrals Session recordings (primarily the educator/lesson feed; see Section 16) Behavioural logs and pastoral notes EBSNA history and relevant context shared at admission

5.2 Parent and Carer Data

Name, contact details, and relationship to the learner Emergency contact information Consent records Billing and invoicing data (where fees are paid by the family)

5.3 Staff, Practitioner, and Contractor Data

Name, contact details, qualifications, and employment history DBS check outcomes and Single Central Record entries Payroll and contractual information Training records and performance data

5.4 Special Category Data

Where NEO processes special category data (for example health information, SEND data, ethnicity), this is done under explicit consent or another Article 9 condition such as safeguarding of children, legal obligation, or substantial public interest.

6. Confidentiality and Privacy

Confidentiality is never absolute where safeguarding concerns exist. The safety of the child always takes precedence. Information is shared on a need-to-know basis and in line with DfE (2018) Information Sharing: Advice for Practitioners

and the seven Caldicott principles. Learners are informed, in age-appropriate ways, that safeguarding may override confidentiality. Personal images, video, or voice recordings are never shared publicly without explicit parental consent. Session recordings primarily capture the educator/lesson feed; if recordings need to be shared for safeguarding reasons, the identity of learners not related to the incident is obscured wherever technically possible. Only secure, approved platforms are used for processing and storing personal data (see Section 7). Termly joint DSL and DPO reviews monitor confidentiality practices and identify any breaches or areas for improvement.

7. Roles and Responsibilities

Role	Responsibility
Proprietor	Named accountable person under OEAS framework; ensures adequate resourcing of the data protection function; receives anonymised reports on data incidents and compliance.
Data Protection Officer (DPO)	Leads on UK GDPR compliance across NEO; primary point of contact for the ICO; advises on Data Protection Impact Assessments (DPIAs); maintains the NEO Record of Processing Activities (ROPA); coordinates breach responses and ICO notifications; conducts termly joint reviews with the DSL. During the initial period the DPO function is held by the Director / Head of School; NEO will review this arrangement as the organisation grows and may appoint an external or dedicated DPO when volume or risk requires it.
Director, NEO & Head of School	Holds the DPO function during the initial period; owner of this policy; escalates significant risks or breaches to the Proprietor.

Role	Responsibility
Designated Safeguarding Lead (DSL)	Ensures safeguarding practice aligns with data protection principles; makes proportionate data-sharing decisions in safeguarding contexts and records the rationale; works with the DPO to review confidentiality and information-sharing practices.
SENCo	Ensures that SEND-related personal data is handled lawfully and that reasonable adjustments do not inadvertently create data protection risks.
All staff, practitioners, contractors, volunteers	Use strong passwords, multi-factor authentication, and secure storage for all personal data; report data incidents immediately to the DPO and DSL; follow guidance on sharing, recording, and storing information securely; never store personal data on personal devices or in personal accounts; complete annual data protection training.

8. Digital Platforms and Data Security

NEO processes personal data across the following approved platforms:

Platform	Purpose	Security Controls
Google Classroom	Curriculum delivery, assignments, resources, learner communication.	Role-based access; managed accounts; assignment privacy settings.
Google Meet	Live lessons, tutorials, pastoral meetings.	Host controls; waiting rooms; recording

Platform	Purpose	Security Controls
		controls; encrypted in transit.
Google Workspace (Gmail, Drive, Docs, Sheets, Forms)	Communication, document collaboration, safeguarding records, registers.	Encrypted at rest and in transit; managed accounts; access controls; audit logs; DLP.
Secure cloud storage	Safeguarding records, EHCP evidence, sensitive files.	Encrypted; access restricted to DSL, DPO, and authorised staff.
Smoothwall	Filtering and monitoring of NEO-managed accounts and enrolled devices for safeguarding (KCSIE 2026).	Data processing agreement in place; alert access restricted to the DSL and designated triage staff; DPIA completed before go-live.

All platforms undergo due diligence review before adoption, including confirmation of data processing agreements, encryption standards, and UK GDPR compliance. Data Protection Impact Assessments (DPIAs) are completed for new or significantly changed platforms.

9. Business Continuity and Platform Resilience

In the event of a platform outage, the following contingency measures apply:

System Affected	Contingency
Google Classroom outage	Asynchronous learning packs distributed via email; assignments collected via Google Forms or Drive.
Google Meet outage	Telephone or approved alternative video platform for urgent pastoral or safeguarding contact; lessons rescheduled.
Google Workspace outage	Encrypted offline backups accessed by senior staff via secure channel; manual logging of safeguarding concerns.

An annual continuity drill is led by the Director / Head of School to test these procedures and identify improvements.

10. Lawful Processing and Consent

All processing of personal data takes place under one or more lawful bases as defined by Article 6 of the UK GDPR: Consent: the individual has given clear, informed consent for processing for a specific purpose. Legal obligation: processing is necessary to comply with the law (for example, safeguarding, tax, employment law). Public task: processing is necessary for the performance of a task carried out in the public interest (for example, education provision). Legitimate interest: processing is necessary for NEO's legitimate interests, provided these are not overridden by the individual's rights. Vital interest: processing is necessary to protect someone's life. Contract: processing is necessary for the performance of a contract (for example, fee payments). For special category data (Article 9), processing occurs under explicit consent or a condition such as safeguarding of children, legal obligation, or substantial public interest. Consent must be freely given, specific, informed, and unambiguous. It can be withdrawn at any time. Where safeguarding applies, consent may be overridden to prevent harm to a child, and the rationale for this decision is recorded.

11. Children's Data and the ICO Children's Code

As a provider serving learners aged 11–18, NEO pays particular attention to the rights of children in relation to their personal data: Privacy notices are written in clear, age-appropriate language, with versions pitched for learners aged 11–13 and 14–18 where helpful. NEO applies the principles of the ICO's Age Appropriate Design Code (Children's Code) to its digital services. Where consent is the lawful basis for processing, learners aged 13 and over may give their own consent for online services in line with UK GDPR provisions. Parental consent is sought for learners under 13 or where otherwise appropriate. Data collection is minimised and default settings are privacy-protective. Learners are supported to understand and exercise their data rights through RSHE and pastoral conversations with their named practitioner.

12. Data Sharing with Local Authorities and Commissioners

Where local authorities or other commissioners fund or refer learners to NEO, NEO will: Share data proportionately: attendance, safeguarding, and progress data is shared securely via agreed channels. Data is minimised and relevant. Provide clear privacy notices: learners, families, and commissioning authorities receive a privacy notice outlining what data is collected, why, and how long it is kept. Establish data processing agreements: NEO recognises that local authorities may act as data controller in some contexts, with NEO as processor, or both as joint controllers. Data processing agreements are put in place where required. Review annually: the DPO reviews data-sharing arrangements with local authorities annually, and immediately following changes to UK GDPR, ICO guidance, or local authority protocols.

13. Individual Rights

Under the UK GDPR, individuals (including learners and parents) have the following rights in relation to their personal data: The right to be informed about data collection and use. The right of access (Subject Access Request). The right to rectification of inaccurate data. The right to erasure (in certain circumstances). The right to restrict processing. The right to data portability. The right to object to processing. Rights relating to automated decision-making and profiling. Requests should be directed to the DPO at

neo@nudgeeducation.co.uk. NEO responds within one calendar month. Subject Access Requests relating to safeguarding records are handled in consultation with the DSL to ensure that disclosure does not compromise the safety of any child.

14. Data Security and Breach Management

NEO takes the security of personal data seriously: All digital data is encrypted at rest and in transit. Access to personal data is restricted on a need-to-know and role-based basis. Staff use strong passwords and multi-factor authentication for all NEO systems. Personal data must not be stored on personal devices or transferred via insecure channels. Periodic access reviews are conducted by the DPO. In the event of a data breach: Contain: immediate steps are taken to contain the breach and limit further exposure. Assess: the DPO and DSL assess the risk to individuals, including any safeguarding implications. Notify: the DPO notifies the ICO within 72 hours where the breach is likely to result in a risk to individuals' rights and freedoms. Affected individuals are informed where the risk is high. Record: all breaches are logged in the NEO Data Incident Register, regardless of severity. Review: root causes are analysed, corrective actions are implemented, and additional training is provided where needed.

15. Safeguarding and Data Protection

Data protection supports safeguarding; it does not limit it. Staff may share information without consent if it is necessary to protect a child from harm. All data-sharing decisions made in safeguarding contexts are recorded, including the rationale and the lawful basis relied upon. Learner autonomy and trauma-informed principles guide all communications about data, ensuring that learners feel respected and informed even when information must be shared. The DPO and DSL conduct termly joint reviews to ensure that data protection practices support, rather than hinder, effective safeguarding.

16. Data Retention

Personal data is retained only for as long as necessary to fulfil the purpose for which it was collected, or as required by law. Indicative retention periods are:

Data Category	Retention Period	Basis
Learner records (general)	Until the learner's 25th birthday	DfE retention guidance.
Safeguarding records	Until the learner's 25th birthday (or longer if required)	KCSIE 2026; local safeguarding partner guidance.
EHCP documentation	Until the learner's 25th birthday	SEND Code of Practice 2015.
Session recordings	Retained for one academic term, unless required for safeguarding	Proportionality and data minimisation.
Staff employment records	Six years after leaving employment	HMRC and employment law requirements.
DBS certificates	Securely destroyed once checked and recorded on the Single Central Record	DBS Code of Practice.
Financial and payroll data	Six years from the end of the financial year	HMRC requirements.

Data that has reached the end of its retention period is securely deleted or destroyed. The DPO conducts an annual review of retained data to ensure compliance.

17. Images, Recordings, and Publication

Session recordings primarily capture the educator/lesson feed and are used for training, quality assurance, and safeguarding. Learner voices and images may be captured incidentally but are not identified or published. Explicit parental consent is obtained before any publication of images, recordings, or

identifying information relating to a learner. Photographs or recordings taken during enrichment activities are governed by the same consent requirements. Staff, practitioners, contractors, and volunteers are prohibited from using personal devices to capture images or recordings of learners.

18. Artificial Intelligence and Data Protection

Where NEO uses AI tools in its operations (see the NEO Online Safety and Acceptable Use Policy), the following data protection requirements apply: No personal data is entered into AI tools unless a DPIA has been completed and the DPO has approved the processing. AI-generated outputs that inform decisions about learners are reviewed by a qualified human professional before use. Learners and families are informed when AI tools are used in ways that materially affect them. AI tools that process personal data must comply with UK GDPR, including data minimisation and purpose limitation. Generative-AI use complies with NEO's agentic-AI design principles, which include identity containment, consent gates, and bounded autonomy — no AI tool may act in ways that materially affect a learner without a human decision-maker in the loop.

19. Monitoring and Review

Joint DSL and DPO reviews of incidents, breaches, and privacy compliance are conducted termly and recorded for governance assurance. This policy is reviewed annually, and cross-checked against the Online Safety and Acceptable Use Policy, cyber security procedures, KCSIE 2026, and OEAS accreditation criteria. An immediate interim review is triggered following updates from the ICO, DfE, NCSC, or changes in statutory guidance. Findings from reviews feed into staff training and system improvements.

Related Policies

This policy should be read alongside: NEO Child Protection and Safeguarding Policy NEO Online Safety and Acceptable Use Policy NEO Behaviour and Regulation Policy NEO SEND Policy NEO Equal Opportunities, Equality and Diversity Policy NEO Admissions Policy NEO Complaints Procedure NEO Terms and Conditions NEO Digital Consent and AI Safety Parent Guide

Document Control

Version	04.26
Approved	April 2026
Next Review	April 2027
Owner	Director, Nudge Education Online & Head of School
Approver	Proprietor
Operating Company	Nudge Education Ltd (Company Number 10192753)

Document control

Field	Value
Version	Dec 2025
Owner	Data Protection Officer
Status	live
Source file	`1. All Company/Data Protection and Information Security Policy - Dec 2025.pdf`