GDPR Policy

Aims

Next Steps Education Ltd takes data protection very seriously. As such, this policy outlines the measures the agency will put in place to ensure the protection of all personal and sensitive data about staff, pupils, parents and other individuals. This policy outlines a data protection by design culture within the agency so that all collection, storage and processing of data, whether digital or on paper, is carried out lawfully in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

Legislation and Guidance

General Data Protection Regulation (GDPR) came into force in May 2018 as part of the Data Protection Act 2018 (DPA 2018) which replaces the previous Data Protection Act 1998. GDPR relates to the collection, processing and storage of personal data. This policy is based on guidance published by the Information Commissioner's Office (ICO) and the ICO's code of practice for subject access requests.

Definitions

Throughout this policy, the following terminology with the accompanying definitions will be used.

Terminology	Definition
processing	Any action or operation performed on personal data, such as, collecting, recording, storing, altering, using, transmitting, destroying or erasing. Processing also includes transferring personal data to third parties.
data subject	Any person about whom we hold personal data. In the case of the school this could relate to pupils, parents, staff, governors, volunteers and visitors.
personal data	Any information that relates to an identified or identifiable (either directly or indirectly), person or data subject.
sensitive data	Relates to a set of special categories that should be treated with extra security. These categories are: · Racial or Ethnic Origin Data · Political Opinions · Religious or Philosophical Beliefs · Trade Union Membership · Genetic Data · Biometric Data
data controller	Any person, agency or authority who decides how and why data is processed. In the case of this policy the school is the data controller.
data processor	Any person, agency or authority that processes data on behalf of a data controller.
data protection officer (DPO)	The person responsible for independent and impartial monitoring and application of laws that protect personal data within the school.
data breach	A breach of security that leads to the accidental or unlawful loss, destruction. alteration, disclosure of or access to personal data while stored, transmitted or being processed must be reported to the Information Commissioner's Office (ICO).
Information Commissioner's Office (ICO)	A UK based organisation responsible for upholding information rights.
data users	Those who process personal data. They must protect data in accordance with this data protection policy.
data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.

Roles and Responsibilities

Next Steps Education Ltd will follow the outline below for distribution of responsibilities in relation to GDPR within the school.

Role	Responsibility
Principal Partners	Ultimate responsibility for GDPR compliance lies with the Principal Partners of Next Steps Education Ltd, Sarah Logan and Liz Fancourt
Tutors	Tutors will not download data from our secure organisational software. Where they make notes and comments about children on paper, these will only use non-identifiable references, such as initials. Tutors agree to store notes within the agency's secure organisational software.
Staff	Staff will not download data from our secure organisational software. Where they make notes and comments about children on paper, these will only use non-identifiable references, such as initials. Tutors agree to store notes within the agency's secure organisational software.
Data Protection Officer (DPO)	The designated Data Protection Officer is Sarah Logan, Principal Partner with Next Steps Education Ltd. As DPO, she is responsible for training tutors and staff on how to comply with GDPR according to our GDPR policy.

Data Protection Principles

The data protection principles that the agency follow in order to be compliant with GDPR state that personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for legitimate purposes;
- relevant and limited to what is necessary in order to fulfil the purposes for which it is processed;
- kept up to date;
- stored for no longer than is necessary;
- processed in a way that ensures it is appropriately secure.

This policy outlines how Next Steps Education will comply with these principles.

Collecting Personal Data

Collecting personal data will be an inevitable part of the day-to-day business of Next Steps Education Ltd. We will only collect personal data for specific, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. To ensure that this data is handled and processed appropriately and with minimal risk, Next Steps Education Ltd, as data controller, adheres to the guidelines outlined below.

Scenario	Procedure
Student Contact Records	Client data (parent or local authority/ school) and relevant pupil records will be held securely on our Tutorcruncher platform. Data is held securely in the cloud and accessible on a need to know basis, ie, tutors can only see the data that the need to see relevant to their pupils.
Student Attendance Records	Pupil attendance will be recorded by tutors within the Tutorcruncher secure platform.
Student Progress Data	Pupil reports will be written by the tutor after each tuition session. These will be written within Tutorcruncher and accessible only to the Principal Partners, the tutor author and the client. Should schools or local authorities wish to have more extensive pupil progress data, this will be held within a secure platform and shared with the relevant parties.
Staff Records	Staff and Tutor records will be held within our secure Tutorcruncher platform. Whilst all tutors and staff must comply with our Safer Recruiting Policy and provide copies of documents with their address, DBS and qualifications, tutors are otherwise responsible for inputting and controlling their own data. Data is only available to the Principal Partners within Next Steps Education Ltd.
Intervention Records	Where necessary, this will be held within the pupil information and accessible as required by staff and tutors.
Special Educational Needs (SEN) Records	Where necessary, this will be held within the pupil information and accessible as required by staff and tutors.
Medical Information and Administration	Where necessary, this will be held within the pupil information and accessible as required by staff and tutors.
Safeguarding Records	Safeguarding concerns, as a YES/NO box after each lesson are held within Tutorcruncher. Any further Safeguarding concerns are kept by our DSL, Liz Fancourt, in a folder locked in an office cabinet.

Sharing Personal Data

As with the collection of personal data, it is integral to the effective functioning of Next Steps Education Ltd that personal data will need to be shared in certain circumstances. To ensure that personal data is shared lawfully, the following considerations must be taken into account.

Scenario	Procedure
Regulatory Bodies e.g. government agencies or healthcare	Before sharing personal data with regulatory bodies requesting access, the DPO will verify the identity of the body and investigate how they intend to use the data shared with them. Only when satisfied with the response will Next Steps Education Ltd share any personal data.
Suppliers or Subcontractors Requiring Access to Personal Data.	The DPO will assess all suppliers and subcontractors' ability to adhere to GDPR. All suppliers and subcontractors requiring access to personal data will read and follow the agency GDPR policy.
The Police	The police will only be able to request access to data with a relevant warrant.

Subject Access Request (SAR)

As part of GDPR, data subjects are entitled to make a request to any organisation, such as Next Steps Education Ltd, to access personal data held about them. This is known as a subject access request (SAR). Next Steps Education Ltd therefore needs to be reasonably prepared for such an eventuality by establishing the procedure outlined below. NB: Personal or sensitive data about a child belongs to the child. However, if a child is deemed unable to understand their rights or the implications of a SAR, or is unable to give consent, a parent or guardian can make the request on their behalf.

Subject Access Request Procedure

1) All staff are trained to recognise a subject access request.
2) Staff involved in responding to a SAR clearly understand the notion of the right to access. They also know when a SAR can be refused and how to act when refusing a SAR.
3) The agency will use the agency specific SAR form. (See appendix 1)
4) Identification of the subject requesting access will be verified.
5) The agency aims to respond to all SARs within one month of submission.
6) Upon receiving a valid SAR, the following procedure will be followed:
   - The staff member who receives the written SAR refers this to the DPO (Sarah Logan).
   - A review of the SAR is carried out in order to establish the exact information requested.
   - The SAR is recorded in the school SAR log and reported to the DPO.
   - The DPO will send a response to the data subject to inform them that their SAR is being processed.
   - The information will be collated and the request responded to.
   - The record on the SAR log is marked as closed.

Photos, Video, Zoom Recordings

Next Steps Education Ltd recognises that photos, video and Zoom recordings of individuals will be part of the personal data processed by the agency. As a result, the following measures are adhered to in order to ensure responsible handling and processing of such data.

Zoom Recordings

- Next Steps Education Ltd uses Zoom recordings in order to keep staff and students safe.
- The agency terms and conditions inform all members of staff and students of how Zoom recordings are processed.
- All Zoom data will be stored for a period of 60 days for security purposes.

Photos and Video

- Photos and videos taken within tuition sessions for public use are to be considered under GDPR.
- Any photo or video of recognisable individuals which the school wishes to publish for example, on the school webpage or social media platform, will only be published with prior written consent. Written consent will be obtained via explicit consent in our terms and conditions
- Photographs and video captured by parents for personal use do not fall under the scope of GDPR.

Data Retention- Security and Storage

At Next Steps Education Ltd only data that is adequate, purposeful, necessary and limited to what is essential will be stored. The school will ensure that any stored data will be protected from unauthorised access and data breaches through the implementation of up to date and well-maintained security protocols. This will guarantee the confidentiality, integrity and availability of personal data. Confidentiality means that data will only be accessed by those who are authorised to access it. The integrity will be maintained through guaranteed accuracy and

suitability of all data stored; inaccurate or unsuitable data will not be retained. Availability will be maintained, meaning those that are authorised to access the personal data are able to do so as and when required.

Specific Data Type	Security Measures
paper records	All paper records taken by tutors will refer only to initials. Only those authorised to access the records will be granted access to the storage location.
portable electronic devices e.g. Laptops, iPads.	Tutors are responsible for their portable electronic devices being password protected. Data will be stored in secure cloud locations.
papers containing personal data e.g. class lists contact sheets	Any paperwork containing personal data will not be left unattended and in sight at any time. Tutors and other staff will ensure that any paper containing personal data will be suitably stored to limit access to the data.
tutor personal devices	Staff will not be permitted to store data on personal devices or store any personal data relating to the school.
sharing with authorised third parties	When required to share data with authorised third parties, the agency and staff will make the necessary checks to guarantee it is handled securely and in line with GDPR.

Staff Remote Working

For remote working to comply with GDPR, Next Steps Education Ltd implements the following procedures:

- All tutor's laptops will be password protected.
- When working remotely and accessing the agency network, staff will use a secure password; this will prevent unauthorised access to agency software and networks.

- Tutors are responsible for having up-to-date antivirus software installed to prevent any malicious or unauthorised access to agency records, personal or sensitive data.
- Staff are permitted to use personal or home Wi-Fi networks but are not permitted to use public Wi-Fi when working remotely. Public Wi-Fi security is not always strong enough to prevent a data breach.

Disposal of Data

Next Steps Education Ltd will always ensure that records containing personal and/or sensitive data are disposed of safely and securely. For example, any paper records due to be disposed of will be securely shredded on site. Any digital records containing personal data will be deleted using the internal erasure procedure of the relevant software. It is up to individuals to make sure they have deleted personal data from devices once that data is no longer relevant, or the device is being passed on.

Compliance Monitoring

As data collection and processing changes and updates. Next Steps Education Ltd confirms continual compliance through compliance monitoring. The designated DPO will, as part of their role, undertake regular monitoring of data records held by the agency, checking they are relevant, necessary and accurate. The DPO will monitor the compliance of the roles outlined in this policy with their assigned responsibilities, impartially checking that these are carried out in accordance with policy. The DPO will monitor who the agency is sharing data with and the integrity and necessity of the third-party data processing. The DPO will monitor procedures for SAR and data breaches, ensuring these are followed correctly and in a timely manner.

Data Breaches

At Next Steps Education Ltd all reasonable action will be taken to keep data handling and processing safe and secure within GDPR. However, should a data breach occur, Next Steps Education Ltd will be prepared to handle any such breach in the manner outlined below. Potential data breaches within an agency context could be an email containing sensitive personal data could be sent to an incorrect email address.

Next Steps Education Ltd Procedure for Handling A Data Breach

- Any potential or confirmed data breach must be reported in the first instance to the DPO.
- Upon receiving notification of a data breach, the DPO will investigate the data breach further to assess the severity of the breach.
- Once the assessment has been made the outcome will be logged by the DPO, whether the breach does or does not need reporting. The log will include the cause of the data breach and any facts surrounding the breach, the effects of the breach and the action taken to minimise risk and prevent a repeat occurrence.
- If the DPO determines that the data breach poses a significant threat to the data subject(s), they will report the breach to the ICO within 72 hours.
- The DPO will attempt to minimise the impact of the breach, supported by relevant parties within the agency.
- Upon receiving the ICO report, the DPO will act upon the ICO's recommendation.

Training

Upon receiving the ICO report, the DPO will act upon the ICO's recommendation.

To guarantee continued compliance with GDPR all staff will receive data protection training as part of the induction process at Next Steps Education Ltd.

Ongoing continuing professional development (CPD) for all staff will include relevant and topical GDPR training as and when required.

Links to Other Policies

The following policies should be read and considered in conjunction with this GDPR policy:
Online Safety Policy

Code of Conduct Policy

Whistle blowing Policy

Safeguarding Policy

Appendix 1

Subject Access Request Form	
Title	
Surname	
First Name(s)	
Date of Birth	
Home Address	
Post Code	
Contact Telephone Number	
Email Address	
Relationship with the agency	Parent / Student / Member of staff / Volunteer / Sub-contractor/ Other If other, please specify:
Identification provided To validate name and address	
Details of data request Please include as much information as possible about the data you are requesting. For example: your personal file, your child's progress data, emails sent between A and B and specific dates.	

I am requesting access to my own personal data, as detailed above. I confirm that I am the individual named above and the data I am requesting access to is my own personal data. I have supplied the information above to aid the subject access request and also to validate my identity. I have provided identification to prove my name and address.

Signature:

Date:

Appendix 2

Data Breach Log Form		
Date of breach		
Date breach was discovered		
Cause of breach		
Description of the breach What happened? Who is involved? Other facts:		
Reported to ICO?	Yes	No
Date reported to ICO (If reported)		
All data subjects informed?	Yes	No
Remedial action		
Follow-up (if required)		
Breach reported by		
Date reported		
Report received by		

Last reviewed: July 2024