GDPR / Data Protection Policy

This is a policy outlining how personal data is collected and managed and what happens in the event of an incident. This policy will be reviewed and updated annually or sooner if legislation changes, or an incident occurs.

Nurture Space Ltd is committed to ensuring that all personal data collected about staff, students, parents, volunteers and other individuals is collected, stored and processed in accordance with UK data protection Law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

policy meets the requirements of:

a. UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

b. Data Protection Act 2018 (DPA 2018) It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

Definitions

a. Personal Data: Any information relating to an identified, or identifiable individual. This may include the individual's:

- Name (Including initials)
- Identification Number
- Location data
- Online identifier, such as a username
- It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

b. Special categories of personal data: Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political Opinions
- Religious or philosophical beliefs
- Genetics

- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – Physical or mental
- Sex life or sexual orientation

Processing: Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.

Data Subject: The identified or identifiable individual whose personal data is held or processed

Data Controller: A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Data Protection Officer: A person responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the organisation's data protection processes and advise on best practice.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Roles and responsibilities

This policy applies to all staff working for or on behalf of Nurture Space Ltd and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Managers Have overall responsibility for ensuring that the organisation and its staff complies with all relevant data protection obligations.

Data Protection Officer: The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities and, where relevant, report their advice and recommendations on the organisation data protection issues.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO. c. All Staff: Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy

- Informing the organisation of any changes to their personal data, such as a change of address.

The DPO for Nurture Space Ltd is Ruth Moor

Contacted via email: ruthmoor22@gmail.com

Contacting the DPO in the following circumstances:

With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Data Protection Principles

The UK GDPR is based on data protection principles that our organisation must comply with. The principles say that personal data must be:

- Processed lawfully, in a transparent way.
- Collected only for specific legitimate reasoning
- Limited to what we deem necessary
- Accurate and up to date
- Kept for no longer than the required need
- Processed to ensure secure

Collecting data

Lawfulness, fairness and transparency: We will only process personal data where we have one of 6 legal reasons to do so under data protection law:

- The data needs to be processed so that the organisation can fulfil a contract with the individual, or the individual has asked the organisation to take specific steps before entering a contract.
- The data needs to be processed so that the organisation can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the organisation can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the organisation or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate) has freely given clear consent.

For special categories of personal data. We will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation.
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a student) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation d. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary. Staff must only process personal data where it is necessary to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

Sharing personal data

We will only share personal data when it is necessary to do so, for the safety of our staff, participants and families. For example:

- A safeguarding concern
- Liaising with other parties (we will ask for consent)
- Printing of documents (we will only use single companies who comply with GDPR)
- Law enforcements where we are legally required to

Data requests

Subject access requests:

Individuals have a right to make a 'subject access request' to gain access to personal information that the organisation holds about them. This includes PR/Data Protection Policy and Guidelines

1. Confirmation that their personal data is being processed

2. Access to a copy of the data

3. The purposes of the data processing

4. The categories of personal data concerned

5. Who the data has been, or will be, shared with

6. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

7. Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing

8. The right to lodge a complaint with the supervisory authority

9. The source of the data, if not the individual 10. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

10. The safeguarding provided of the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

1. Name of individual

2. Correspondence address

3. Contact number and email address

4. Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students on our programme may be granted without the express permission of the student.

This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request.

Responding to subject access requests:

When responding to requests we:

1. may ask the individual to provide two forms of identification

2. may contact the individual via phone to confirm the request was made

3. will respond without delay and within 30 days of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)

4. will provide the information free of charge

5. may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information if it:

1. might cause serious harm to the physical or mental health of the student or another individual

2. would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

3. would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it

4. is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or that they can enforce their subject access request right through the courts.

Other data protection rights of the individual:

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 5), individuals also have the right to:

1. withdraw their consent to processing at any time

2. ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)

3. prevent use of their personal data for direct marketing

4. object to processing which has been justified on the basis of public interest, official authority or legitimate interests

5. object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

6. be notified of a data breach in certain circumstances

7. make a complaint to the ICO

8. ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Photographs and videos

Any photographs and videos taken by parents/carers at our events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this. Where we take photographs and videos, uses may include:

• Within our company including social media campaigns, flyers and other promotional aspects.

• Outside of our premises by external agencies such as newspapers and campaigns

• Online on our website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. We provide our staff with guidelines on the use of images within the ICT and online safety policy.

Security and storage

Staff are expected to store and secure data in alignment with the Nurture Space policy, we adhere to:

A: protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

B: Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

C: Passwords that are at least 10 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals

D: Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

E: The google drive of the company will remain secure and password protected, requiring two form authentications to gain access, granted only by the GDPR lead.

Disposal

Data that is no longer needed for Nurture Space purposes will be removed in due course, this will be shredding of paper copies, and removal of all electronic trails or copies.

Breaches

We will work closely with all parties to ensure data breaches are unlikely to occur, if they do occur, we will report this directly to the ICO within 72 hours, ensuring we are following national protocol.

Training

All staff are required read and sign the data protection policy, while agreeing to undertake any upskill of qualifications deemed necessary by Nurture Space Ltd.

Monitoring

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually unless legislation requires otherwise and approved by the Managers.

Policy dated: August 2024

Review date: August 2025

Authorised by: Ruth Moor (Director of Nurture Space Ltd)

Signed: