Version	Adopted by Board on	Signature of Chair
1.0	27.09.19	

TURN EDUCATION
ANIMAL ASSISTED LEARNING

Data Protection Policy

Contents

1. Aims

Our organisation aims to ensure that all personal data collected about staff, children who use our services and those who have parental responsibility for them (referred to in this document as 'parents') and/or their nominated contacts, along with directors, employees, workers and any volunteers who may work with us from time to time, are collected, stored and processed in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether in paper or electronic format.

Readers of this policy are asked to be aware of the relatively small size of the organisation and, therefore, the inevitable constraints on the organisational, financial and technological capabilities and capacity of the organisation, when interpreting the various clauses of the policy.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's Code of Practice for subject access requests.

It also reflects the ICO's Code of Practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
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.
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 ● Trade union membership ● 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 individuals 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Organisation	TURN Education C.I.C.

4. The Data Controller

Our organisation processes data relating to parents (and/or their nominated contacts), children who use our services, staff, directors, volunteers, visitors and others and, therefore, is a Data Controller.

The organisation understands that, as a not-for-profit organisation it is not currently required to register with the ICO. This situation will be regularly reviewed.

5. Roles and responsibilities

This policy applies to all directors, staff, employees, workers and volunteers employed by or working with our organisation and also to external organisations and/or individuals working on our behalf. Directors, staff, employees workers and volunteers who do not comply with this policy may face disciplinary action as defined in *'Putting Things Right'* the organisation's disciplinary framework.

5.1 Board of Directors

The Board of Directors have overall responsibility for ensuring that our organisation complies with all relevant Data Protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with Data Protection legislation and developing related policies, procedures and guidelines where applicable.

The DPO will report to the Board of Directors on a regular basis (and, at least, annually) on matters relating to Data Protection and provide advice and recommendations on any Data Protection issues.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO.

Our Data Protection Officer is **Caroline Hardeman-Mason.** She can be contacted at Caroline.hardemanmason@turneducation.co.uk 07734 543827

5.3 Managing Director

The Managing Director acts as the representative of the Data Controller on a day-to-day basis.

5.4 All staff*

** for the purposes of this policy, the term 'staff' is intended to include directors, employees, workers, consultants, contractors and volunteers and anyone working for, or under the direction of, TURN Education C.I.C.*

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 (but only if the organisation currently holds personal data relating to the individual concerned)
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, Data Protection legislation, the retention of 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 European Economic Area
    - If there has been a data breach
    - Whenever they are engaged 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

6. Data Protection principles

The GDPR are based on Data Protection principles with which our organisation must comply.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which they are processed
- Processed in a way that ensures they are appropriately secure

This policy sets out how the organisation aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to so under Data Protection legislation:

- 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** (this basis is unlikely to apply to this organisation)

- 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, in particular where the Data Subject is a child)
- The individual (or their parent where appropriate in the case of a child) has freely given clear **consent**

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

Although the organisation has no current plans to do so, if we offer online services to our service users, such as apps or similar, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 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 the data, 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 in order to do their jobs/complete their allotted tasks.

When staff no longer need the personal data they hold, they must ensure it is deleted or, where applicable, anonymised.

8. Sharing personal data

We will not normally share personal data with anyone else but may do so where:

- There is an issue with a child or parent/nominated contact that puts the safety of our staff at risk
- We need to liaise with other agencies - we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and service users - for example, I.T. companies. When doing this, we will:
  - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with Data Protection legislation
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a stand-alone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data are sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our service users or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with Data Protection legislation.

9. Subject access requests and other rights of individuals

9.1 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:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of the personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or, if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data and what the significance and consequences of this might be for the individual

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

- Name of individual

- Correspondence address
- Contact number and email address
- Details of the information requested

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

9.2 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 as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers may be granted without the express permission of the child concerned. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via telephone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within three months of receipt of the request where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning a child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

9.4 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 7) individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- 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.

10. Personal Development and Achievement Plans

Parents, or those with parental responsibility, will be allowed to access their child's Personal Development and Achievement Plan provided a written request is made to the DPO. Personal Development and Achievement Plans may also be shared with Social Workers and other professional bodies if they have been involved with referring the child to the organisation.

11. CCTV

Although, as an organisation, we do not currently use CCTV on our site, we reserve the right to do so in the future. If we do choose to utilise CCTV at any time on our site, we will do so primarily to ensure that our site remains a safe environment for staff, children, parents and visitors. We will adhere to the ICO's Code of Practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV but we will make it clear where individuals are being recorded. Security cameras will be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system (when a CCTV system is operational) should be directed to the DPO.

12. Photographs and videos

As part of our organisational activities, we may take photographs and record images of children using our service.

We will obtain written consent from parents (or those with parental responsibility) for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent (or someone with parental responsibility) and pupil.

Uses may include:

- Within the organisation on notice boards and within in-house magazines, brochures, newsletters etc.
- Outside of the organisation by external agencies such as a photographer commissioned by the organisation to take images of children, funding agencies, newspapers, campaigns
- Online on our organisation's website

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.

13. Data Protection by design and default

We will put measures in place to show that we have integrated Data Protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO and ensuring that they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing data that is necessary for each specific purpose of processing and always in line with the Data Protection principles set out in relevant Data Protection legislation (see Section 6)
- Completing Privacy Impact Assessments where the organisation's processing of personal data presents a high risk to the rights and freedoms of individuals and when introducing new technologies (the DPO will advise on this process)
- Integrating Data Protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on Data Protection legislation, this policy, any related policies and any other Data Protection matters. A record of any such training will be maintained
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of Data Subjects, making available the name and contact details of our organisation and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, Data Subject, how and why we are using the data, any third party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14. Data security and storage of records

We will 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives **that contain personal information** will be kept under lock and key when not in use
- Papers containing confidential personal information will not be left or displayed anywhere where there is general access
- Where personal information needs to be taken off-site, staff must maintain a record of the information transported and the date, time, duration and location of the period when the information was off-site.
- As a matter of organisational policy, passwords containing at least 8 characters comprising letters and numbers will be used to access the organisation's computers, laptops and other electronic devices. Staff and children using the organisation's computers laptops and other electronic devices, will be reminded to change their passwords at regular intervals
- Staff and children who store personal information on their personal devices will be expected to follow, as a minimum, the same security procedures as for organisation-owned equipment. However, staff and children should not store personal information which has been properly provided to the organisation.
- Where we need to share personal data with a third party, we will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see Section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the organisation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with Data Protection legislation.

16. Personal data breaches

The organisation will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours.

17. Training

All staff will be provided with Data Protection awareness training as part of their induction process.

Data Protection will also form part of the Continuing Professional Development (CPD) of members of staff where changes to legislation, guidance or the organisation's processes make this necessary.

18. Monitoring arrangements

The DPO, in conjunction with the Board of Directors, is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated (where necessary) at least 12 months after the adoption of this policy and thereafter as determined by the Board of Directors.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach or potential breach, the staff member or Data Processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available when it should not have been
  - Made available to unauthorised persons
- The DPO will alert the Chair of the Board of Directors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or Data Processors where applicable and necessary (actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are and how likely they are to happen
- The DPO will consider whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms and cause them any physical, material or non-material damage (e.g. emotional distress) including through:
  - Loss of control over their data

- Discrimination
- Identity theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be stored on the organisation's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of the individuals concerned
    - The categories and approximate number of the personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons

why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data have been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals - for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Reports of all breaches will be stored on the organisation's computer system.

The DPO and the Board of Directors will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably practicable.