One Education Ltd
Data Protection Policy

OneEducation
Putting children first

Approved by:	Executive Team	**Date:** 15.10.20
Last reviewed on:	N/A	
Date of next review:	October 2022	
Version:	V2.3	

Contents

1. Aims 4
2. Legislation and guidance 4
3. Definitions 4
4. Data Controller and Data Processor 5
5. Roles and responsibilities 5
6. Data protection principles 7
7. Collecting personal data 7
8. Sharing personal data 8
9. Subject access requests and other rights of individuals 8
10. Data protection by design and default 10
11. Data security and storage of records 11
12. Disposal of records 11
13. Personal data breaches 11
14. Training 12
15. Monitoring arrangements 12
Appendix 1: Personal data breach procedure 13

1. Aims

One Education Ltd aims to ensure that all personal data collected about staff, from clients and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of 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.

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

4. Data Controller and Data Processor

One Education Ltd processes personal data for many reasons, including in relation to the services it provides and in its role as an employer. In most instances One Education Ltd will be the data controller (usually alone, but sometimes jointly) in respect of the personal data it processes (i.e. it will determine the purpose and means of the processing); on occasion it may act as a data processor on behalf of another data controller.

One Education Ltd is registered as both a data controller and data processor with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** working for One Education Ltd, and to external organisations or individuals working on our behalf.

5.1 Executive Team

The Executive Team has overall responsibility for ensuring that One Education Ltd 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 One Education Ltd and its staff's compliance with data protection law, and developing related policies and guidelines where applicable.

Advising on data protection impact assessments.

Training staff and conducting internal audits.

The DPO will provide an annual report of their activities directly to the Senior Management.

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

One Education Ltd will ensure that:

- The DPO reports to the Executive Team in respect of their duties as DPO.
- The DPO operates independently and is not dismissed or penalised for performing their task.

Our DPO is contactable via dpo@oneeducation.co.uk.

5.3 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing One Education Ltd of any changes to their personal data, such as a change of address
- Reporting any actual or suspected data breach and cooperating with the DPO thereafter.
- 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 there has been a data breach

Team Leaders are responsible for:

- Developing data sharing protocols which meet the operational requirements of the service and meet DP requirements
- Evaluating the impact on individual data rights before they are engaging in a new activity that may affect the privacy rights of individuals
- Contacting the DPO if they need help with any contracts or sharing personal data with third parties
- Ensuring team members are aware of and follow the team's current data security, handling and storage protocols
- Assisting the DPO in the event of a data breach as set out in Appendix 1

5.4 Disciplinary action and criminal offences

Serious breaches by staff of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action including dismissal and may even give rise to criminal offences.

6. Data protection principles

The GDPR is based on data protection principles that One Education Ltd must comply with.

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 it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how One Education Ltd aims to comply with these principles.

7. Collecting personal data

One Education Ltd processes personal data for many reasons, including in relation to the services it provides and in its role as an employer.

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

a) The data needs to be processed so that One Education Ltd can **fulfil a contract** with a client, or a client has asked One Education Ltd to take specific steps before entering into a contract

b) The data needs to be processed so that One Education Ltd can **comply with a legal obligation**

c) The data needs to be processed to ensure the **vital interests** of a data subject (e.g. to protect someone's life)

d) The data needs to be processed so that One Education Ltd can perform a task **in the public interest**, and carry out its official functions

e) The data needs to be processed for the **legitimate interests** of a data subject or a third party (provided the individual's rights and freedoms are not overridden)

f) A data subject 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 Data Protection Act 2018.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons connected with the provision of our services.

Staff must only process personal data where it is necessary in order to do their jobs.

When receiving personal information from a data controller (e.g. local authority, school, outside agency), it will be their responsibility to inform data subjects that their data has been shared with One Education.

8. Sharing personal data

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

- We need to liaise with external agencies – we will seek consent if necessary before doing this.
- One Education Ltd may also, in appropriate circumstances, make discretionary disclosures of personal data to a person or organisation other than the data subject where it is permitted to do so by law. When deciding whether to exercise its discretion to disclose personal data in such circumstances One Education Ltd will always give proper consideration to the data subject's interests and their right to privacy.
- External agencies, companies, individuals, suppliers or contractors ("third parties") undertaking processing of personal data on behalf of One Education Ltd need data to enable us to provide our services. When working with third parties, we will:
    - Only appoint third parties who can provide sufficient guarantees that they comply with data protection law
    - Only share data that the third party needs to carry out its service.
- 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 is sufficiently anonymised or consent has been provided.
- We are asked to assist emergency services and/or local authorities to help them to respond to an emergency situation.

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 One Education Ltd 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 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, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested
- Details of the preferred format in which any information disclosed to the data subject should be provided in.

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

9.2 Responding to subject access requests

When responding to requests, we:

- Where necessary, will ask the individual to provide 2 forms of identification and/or will contact the individual via phone to confirm the authenticity of the request.
- Where applicable, will ask for the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative or authorised agent).
- Will provide the information free of charge
- Will respond without undue delay and in any event within one calendar month, subject to the following two exceptions:
    - Where further time is necessary, taking into account the complexity and the number of the request(s) from the data subject, the period for responding will be extended by up to two further calendar months. Where such an extension is required One Education Ltd will notify the data subject that this is the case within one calendar month of receiving their request.
    - Where the request(s) from a data subject are manifestly unfounded or excessive (in particular because of their repetitive character) One Education Ltd will ordinarily refuse the request(s). In exceptional cases One Education Ltd may instead exercise its alternative right in such circumstances to charge a reasonable fee that takes into account the administrative cost of complying with the request.

Data protection law allows exemptions from complying with data subject rights in specific and limited circumstances. One Education Ltd will normally apply the exemptions where they are engaged, unless it is satisfied that it is appropriate or reasonable not to do so.

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

9.3 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, 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.

One Education Ltd recognises the fundamental nature of the individual rights provided by data protection legislation. One Education Ltd will ensure that all valid requests from individuals to exercise those rights are dealt with as quickly as possible and by no later than the timescales allowed in the legislation.

10. Data protection by design and default

One Education Ltd has put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal 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 law (see section 7.1)
- Completing privacy impact assessments where One Education Ltd's processing of personal data presents a high risk to 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 law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

- 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 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

11. 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 data are kept secure when not in use
- Papers containing confidential personal data must not be left on office desks, pinned to notice/display boards, or left anywhere else where there is general access
- Secure passwords are used to access office computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff are asked not to store personal information on their personal devices
- 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 (see section 8)

12. Disposal of records

Personal data that is no longer needed is disposed of securely.

Personal data that has become inaccurate or out of date is disposed of securely, where we cannot or do not need to rectify or update it.

For example, we shred paper-based records, and overwrite or delete electronic files.

Where we use a third party to safely dispose of records on One Education Ltd's behalf we will require the third party to provide sufficient guarantees that it complies with data protection law.

13. Personal data breaches

One Education Ltd will ensure that individuals handling personal data will be trained to an appropriate level in the use and control of personal data.

One Education Ltd will ensure that all staff handling personal data know when and how to report any actual or suspected data breach, and that appropriately trained staff manage any breach correctly, lawfully and in a timely manner.

Breaches will be reported to the ICO where such reporting is mandatory or otherwise appropriate and shall be done within the required timescales.

14. Training

All staff are provided with data protection information as part of their induction process.

Data protection will also form part of regular continuing professional development, including but not limited to when there are changes to legislation, guidance or our processes.

The DPO will monitor completion rates of data protection courses to ensure that all staff are appropriately trained.

In addition to the basic training, some post-holders may be required to undertake further information governance or data protection training where appropriate for a particular role or within a specific service area.

15. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years.

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 where it should not have been
    - Made available to unauthorised people
- The DPO will advise the Executive Team that there has been a data breach
- 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 necessary.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out 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
    - Identify 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's 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.
- Where the ICO must be notified, the DPO will do this 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 individuals concerned
        - The categories and approximate number of 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 Team Leader will promptly inform all individuals whose personal data has 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 Team Leader 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)
- The DPO will meet with Senior Management to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.