Inclusion is at the
heart of our trust

Data Protection Policy

Oak
Learning Partnership

Oak Learning Partnership Document: Data Protection Policy

Author:	Data Protection Officer (DPO)
Approver:	Trustees
Owner:	CFO
Date:	March 2023
Next review:	March 2024

Changes History:

Version	Date	Amended by:	Substantive changes:	Purpose
1.0	May 2022	CFO	New document	First release
2.0	March 2023	DPO	Appendix 1 added	Review

Table of Contents

1. Purpose of the Policy

Oak Learning Partnership ('the trust') aims to ensure that all personal data collected about staff, pupils, parents, trustees, QEB members, visitors and other individuals is collected, stored and processed in accordance with the United Kingdom General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy sets out the measures taken to help ensure that this is achieved. It applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legal Background

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

The regulation provides a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed, retained, deleted or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration and disclosure.

3. Definitions

3.1 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.

3.2 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

3.3 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.

3.4 Data subject
The identified or identifiable individual whose personal data is held or processed.

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

3.6 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.

3.7 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. The Data Controller

The trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The trust delegates the responsibility of the data controller to the employees of the trust.

The trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to **all staff** employed by the trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trust Board
The Trust Board has overall responsibility for ensuring that our trust 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 law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trustees and, where relevant, report to the board their advice and recommendations on trust data protection issues.

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

Our DPO is Sheryl Cardwell and is contactable via dpo@oaklp.co.uk

6. Data Protection Principles

The GDPR is based on data protection principles that the trust 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 the trust 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 do so under data protection law:

- The data needs to be processed so that the trust can **fulfil a contract** with the individual, or the individual has asked the trust to take specific steps before entering into a contract
- The data needs to be processed so that the trust 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 trust, as a public authority, 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 trust or a third party (provided the individual's rights and freedoms are not overridden)

The individual (or their parent/carer when appropriate in the case of a pupil) 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 article 9 of the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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 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 in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Records Management and Retention Schedule.

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 pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent when necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone 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 is 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 pupils 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 law.

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 trust 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 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 aged 12 and above are generally 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 pupils at trust schools may not be granted without the express permission of the pupil. This is not a rule and a pupil'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 2 forms of identification
- May contact the individual by phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil 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 the 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 8), 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. CCTV

We use CCTV in various locations around the trust site to ensure it remains safe. 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 make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO, Mrs Sheryl Cardwell dpo@oaklp.co.uk

11. Photographs and videos

As part of our trust activities, we may take photographs and record images of individuals within our grounds or whilst on Trips and Visits.
We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within the trust on school notice boards and in trust or school magazines, brochures, newsletters, etc.
- Outside of trust schools by external agencies such as trust or school photographers, newspapers, campaigns
- Online on our school or trust websites 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.

12. 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 they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only process 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 6)
- Complete privacy impact assessments where the trust'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)
- Integrate data protection into internal documents including this policy, any related policies and privacy notices
- Regularly train members of staff on GDPR legislation, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conduct 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 trust and schools 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

13. 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 under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the main office
- Passwords that are at least 8 characters long containing letters and numbers are used to access trust or school computers, laptops and other electronic devices. Staff and pupils are required 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, pupils or Trustees should not store personal information on their personal devices. Staff should use their own devices to do, or obtain prior consent from the ICT Support Team, should this be required for specific activities. Trustees must adhere to the same security procedures as for trust or school owned equipment for managing any personal information.
- 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 7)

14. 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 schools' or trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with GDPR regulation.

15. Personal data breaches

The trust 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. Such breaches in a trust or school context may include, but are not limited to:

- A non-anonymised dataset being published on the trust or schools websites which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a trust or school laptop containing non-encrypted personal data about pupils

Appendix 1

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

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. So, a data breach has occurred if personal data has been lost, stolen, destroyed (accidentally or in error), altered (accidentally or in error), disclosed accidentally or in circumstances where it should not have been or otherwise made available to unauthorised people.

Step 1: On finding or having caused a data breach, staff members or third-party data processors must notify the Data Protection Officer immediately.

Step 2: The DPO must notify the CFO immediately when notified of a breach.

Step 3: The DPO will take all reasonable steps to contain the breach and minimise its effects as far as possible, requesting action from staff members and any third-party data processors that may be required.

- Can the data be retrieved or safely deleted/destroyed by any unintended recipient(s)?
- Are we certain we have identified all the data that was lost/mistakenly disclosed or altered etc?

Step 4: At the earliest possible time, the DPO will assess the potential consequences of the breach. The DPO should consider;

- How could it affect the data subject(s) involved?
- How serious will these effects be for the data subjects?
- How likely is it that the data subjects could be affected in this way(s)?

Step 5: The DPO must decide whether or not the breach must be reported to the ICO. Breaches must be considered on a case-by-case basis; however, a breach must be reported to the ICO if it is likely to result in any physical, material or non-material damage such as;

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation
- damage to reputation
- or any other significant economic or social disadvantage to the

individual(s) concerned

If the breach is likely to affect anybody in any of the ways described above, and cannot be successfully contained or rectified, it must be reported to the ICO.

Step 6: The DPO will document the decision taken as to whether or not the ICO are notified of the breach. The school should keep a record of this decision in case it is challenged at a later date by any of the individuals involved or by the ICO. The school should keep a record of breaches whether or not they are reported to the ICO. This record should include:

- A description of the breach and how it occurred
- Details of the data involved
- A description of the potential consequences of the breach
- Details of how likely it is any individuals could be affected
- A description of measures taken to contain or rectify the breach
- Actions taken to avoid any repeat of errors that lead to the breach

Step 7: In cases where the breach must be reported to the ICO, the DPO (or another member of staff if they are not available) must do so within 72 hours of becoming aware of the breach. Such breaches are reported via the relevant page on the ICO's website.

Step 8: The DPO must decide whether or not the individual's affected by the breach must be notified. Again, the potential risks to any affected individuals (described in Step 5), the severity of any affects and the likelihood of them being affected must guide this decision-making process. If there is a high risk the DPO will notify, in writing, all potentially affected individuals. This notification will include:

- Contact details for the DPO
- A description of how the breach occurred and the data involved
- A description of the measures taken to contain or rectify the breach
- Any advice it is possible to provide in terms of how the individuals could be affected

Step 9: The DPO must ensure records of breaches and decisions taken relating to them are stored and accessible in the event of any subsequent investigation by the school or the ICO.