



Data Protection Policy

November 2025

Written by:	Anita Breeze
Approved by:	Board of Trustees
Date Approved:	November 2025
Date of Review:	November 2026 (sooner if PHP update)
Version:	5

Contents

1.	Introduction.....	3
2.	What is the General Data Protection Regulation (UK GDPR)?.....	3
3.	Who does it apply to?	3
4.	What is Data?	3
5.	What are the key principles of the UK GDPR?.....	4
6.	Who is a 'data subject'?	5
7.	Data subjects' rights.....	5
8.	Subject Access Requests.....	5
9.	Who is a 'Data Controller'?.....	6
10.	Who is a 'Data Processor'?	6
11.	Processing data	7
12.	Data Sharing	7
13.	Breaches & Non Compliance	8
14.	Consent.....	8
15.	Consent and Renewal	8
16.	For Pupils and Parents/Carers	8
17.	Pupil Consent Procedure	9
18.	Withdrawal of Consent	9
20.	Data Protection Officer	9
21.	Physical Security	10
22.	Secure Disposal	10
23.	Complaints & the Information Commissioner Office (ICO).....	10
24.	Monitoring and Review.....	11

Appendix A Complaints Process

Appendix B Complaints Form

1. Introduction

Odyssey Collaborative Trust are committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

Each school will be responsible for the day to day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

The trust central team are responsible for data held centrally about individuals.

Where we use the phrase 'we' that refers to the trust and the individual schools.

2. What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

3. Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and provisions in the Data Protection Act 2018.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

4. What is Data?

Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This

is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Privacy Notices that explain how data about specific groups or activities is used and stored are also available. These can be obtained from each school and links on the website to UK GDPR compliance.

5. What are the key principles of the UK GDPR?

Lawfulness, transparency and fairness

The Trust must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent we have a form to complete to allow us to process your request. There are some times when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.

Retention

A retention policy is in place that governs how long records are held for.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Details are included in the Trust Acceptable Use Policy, Information Security Policy and Records Management Policy which are all available on the Trust Website.

6. Who is a 'data subject'?

An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

7. Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

These Data Subject's Rights are set out in more detail in the document 'My Rights – A Guide for Data Subjects'.

8. Subject Access Requests

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In accordance with the Data (Use and Access) Act 2025, we are required to conduct searches that are reasonable and proportionate when responding to a SAR. If a request results in a substantial volume of data deemed to be unreasonable and disproportionate, we will notify you and offer an opportunity to refine the scope of your request. This allows you to specify the information you are seeking, enabling us to carry out a targeted search and provide the most relevant data.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information by paper or electronic form.

If you wish to complain about the process, please see Appendix A and B included in this policy.

9. Who is a 'Data Controller'?

The Trust is the Data Controller. They have ultimate responsibility for how the schools and trust central team manage data. They delegate this processing to individuals to act on their behalf, that is the trust central team and the relevant school staff in each setting.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

As the Data Controller, individuals process data on behalf of the organisation. This can be a member of staff, possibly a governor or trustee, a consultant or temporary employee.

10. Who is a 'Data Processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected.

Data Controllers must make sure that Data Processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

11. Processing data

The Trust and the schools must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR as amended by the Data (Use and Access) Act (DUAA) 2025 has seven conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.
- to safeguard vulnerable individuals, crime prevention, and respond to emergencies.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

12. Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

13. Breaches & Non Compliance

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed.

Protecting data and maintaining Data Subjects' rights is the purpose of this policy and associated procedures.

14. Consent

As a Trust, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

This will largely be managed in individual schools.

15. Consent and Renewal

On the School and Trust websites we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail: <https://www.odysseyct.org.uk/gdpr/>

Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

16. For Pupils and Parents/Carers

On joining the school, you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form are reviewed on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available. This is the obligation of each individual to notify the school of changes.

17. Pupil Consent Procedure

Where processing relates to a child under 13 years old, it is typical for an organisation to obtain consent from a person who has parental responsibility for the child as required. All of our pupils are under the age of 13, so consent will always be sought.

18. Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form.

19. CCTV Policy

Please also see the CCTV and IT Security policy. We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:

- detection and prevention of crimes, in the school/academy and on the premises
- student behaviour management, discipline and exclusions
- staff disciplinary and associated processes and appeals
- maintaining a safe environment for the whole school community

20. Data Protection Officer

We have a Data Protection Officer (DPO) whose role is: -

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- to monitor compliance with the UK GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- To be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the UK GDPR

Our DPO is John Walker whose contact details are below:

Address: The Brutus Centre, Station Road, Totnes, Devon, TQ9 5RW

Email: info@phplaw.co.uk

21. Physical Security

As a **Trust** we are obliged to have appropriate security measures in place.

In the Trust, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Site Manager/supervisor is responsible for authorising access to secure areas along with the Senior Leadership Team and Business Manager.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have the suitable security and review measures in place.

22. Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

23. Complaints & the Information Commissioner Office (ICO)

In accordance with requirements set out by DUAA 2025, Odyssey Collaborative Trust has established a dedicated complaint procedure for data protection matters. Please refer to, Appendix A in this Policy.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis in the first instance. If the informal process is unsuccessful or deemed inappropriate, please complete our dedicated form (Appendix B), and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk

Helpline: 0303 123 1113

Website: www.ico.org.uk

24. Monitoring and Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the COO in the Central Team every 12 months, sooner if guidance changes as suggested by PHP Law. This is also monitored and overseen by the Board of Trustees.

Data (Use and Access) Act 2025 - Complaint Process Appendix

Introduction

Odyssey Collaborative Trust is committed to protecting the privacy and personal data of its students, staff, parents/carers, governors and the wider school community. This policy outlines the procedure for handling complaints related to data usage and access, in accordance with the Data Usage Access Act (DUAA) and other relevant UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The UK GDPR documents as set out on our website provide an overview of how personal data is managed across our settings.

This is an appendix to the main complaint policy and reflects the requirement for standalone data usage complaints to be handled using a separate procedure. Any complaint that is linked to other matters whether raised as a formal or informal complaint are to be dealt with under the standard complaint process as outlined within the main complaint policy.

Roles and responsibilities

The Data Controller (DC) is responsible for ensuring compliance with this policy and the legal obligations imposed by the UK GDPR, Data Protection Act 2018, Data Usage and Access Act 2025 and other relevant legislation. The DC will delegate day to day management of this to the relevant staff member and the DC will expect that staff member to investigate any complaint unless there is a conflict of interest, in which case the DC will appoint a suitable person.

The headteacher and leadership team are responsible for ensuring all staff are aware of this policy and their data protection obligations.

All staff members are responsible for handling personal data in a secure and lawful manner and for co-operating fully with any investigation into a data usage or access complaint.

Scope

This policy applies to all individuals who have dealings with Odyssey Collaborative Trust and believe that their personal data has been used or accessed inappropriately, or that their rights under the DUAA and other data protection laws have been infringed.

This includes but is not limited to:

- current and former students
- parents/carers
- school staff (teaching, support, and administrative)
- governors
- volunteers
- contractors and suppliers

Principles

Fairness and transparency: All complaints will be handled in a fair, impartial, and transparent manner.

Confidentiality: Complaints and all related information will be treated with the utmost confidentiality, unless disclosure is required by law.

Timeliness: Complaints will be acknowledged and investigated in a prompt manner.

Compliance: All actions taken will comply with the DUAA, UK GDPR, DPA 2018, and other relevant legislation.

The complaint procedure

Step 1: Informal resolution

We encourage individuals to first attempt an informal resolution of their concerns. If you have a concern about data usage or access, you should, in the first instance, raise it with the relevant GDPR Lead in your school/organisation. (Business Manager if school, COO if Central Team)

In many cases, issues can be resolved quickly and informally at this stage.

Step 2: Formal complaint submission

If the informal approach is not successful or deemed inappropriate, a formal complaint should be submitted in writing using the complaint form attached.

The complaint should be addressed to the GDPR Lead as indicated above.

The written complaint should be made on the form included with this Policy Appendix B. Or shall include the following information:

1. your full name and contact details.
2. a clear and concise description of the complaint, including what happened, when it happened, and who was involved.
3. a description of the data involved and how you believe it was used or accessed inappropriately.
4. any relevant dates, times, or evidence.
5. details of any informal steps you have already taken to resolve the issue.
6. the desired outcome of the complaint.

Step 3: Acknowledgment and investigation

You will receive an acknowledgment of the written complaint within 5 working days of the setting receiving it.

The DC will conduct a thorough and impartial investigation into the complaint.

This may involve:

- interviewing the complainant

- interviewing relevant staff members
- reviewing school records, logs, and policies
- consulting with external legal or data protection experts if necessary

The school/trust will aim to complete the investigation and provide a substantive response within 20 working days of the complaint's acknowledgment. If the investigation is complex and requires more time, the DC will write to the complainant to explain the reason for the delay and provide a new estimated completion date.

Response

The DC will provide a formal written response to the complainant.

This response will include:

- the findings of the investigation.
- a clear and reasoned conclusion as to whether the DUAA or other data protection laws have been breached.
- details of any corrective action taken or planned to prevent a recurrence of the issue.
- the outcome of the complaint, including whether it has been upheld, partially upheld, or not upheld.
- information on the next steps available to the complainant if they remain dissatisfied.

Escalation

If the complainant is not satisfied with the final response, they have the right to escalate their complaint to the Information Commissioner's Office (ICO).

The ICO's contact details are as follows:

Website: <https://ico.org.uk>

Telephone: 0303 123 1113

Postal Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Data (Use and Access) Act 2025 – Complaint Form

To be completed by the complainant

Please return this form to GDPR Lead in your School - School Business Manager (COO if Central Team)

Part 1: Complainant's Details

Please provide your full contact information so we can communicate with you regarding your complaint.

Full Name:	
Relationship to the trust/school: (e.g. student, parent/carer, staff member, former student, volunteer, contractor)	
If student:	
year group:	
form/class:	
If parent/carer:	
student's full name:	
student's year group:	
Contact telephone number:	
Email address:	
Postal address:	
Preferred method of contact: (e.g. email, phone or post)	

Part 2: Details of the complaint

Please provide a clear and concise description of your complaint.

Date(s) of the incident(s)	
When did the misuse occur or when did you become aware of it?	
Nature of the complaint	
Please tick all that apply and provide details below:	
Unauthorised access to personal data	
Unauthorised disclosure of personal data	
Incorrect or inaccurate personal data	
Unlawful processing or use of personal data	

<p>Failure to respond to a data subject request</p> <p>e.g. Subject Access Request or Right to Erasure</p>	
Other (please specify)	
Description of the incident(s)	
<p>What happened?</p> <p>Provide a detailed narrative of the events.</p>	
<p>Who do you believe was involved?</p> <p>e.g. specific staff member, department, external party</p>	
<p>What personal data was involved?</p> <p>e.g. name, address, medical information, academic records, disciplinary records, financial details, sensitive personal data</p>	
<p>How do you believe your data was misused or accessed inappropriately?</p>	
<p>Where did the incident occur (if applicable)</p>	
<p>Has there been any previous attempts to resolve this issue informally?</p> <p>e.g. discussed with a teacher, GDPR lead, head of department.</p>	Yes or No
<p>If yes, please provide details of who you spoke to and when.</p>	

--	--

Part 3: Supporting evidence

Please list and attach any evidence that supports your complaint. This could include:

- emails or correspondence
- screenshots
- dates and times of relevant events
- witness statements (if applicable)

Please list attached documents here:

Part 4: Desired outcome

Please specify the resolution that you are seeking as a result of this complaint?

<input type="checkbox"/>	Investigation and explanation of what happened
<input type="checkbox"/>	Correction of inaccurate data
<input type="checkbox"/>	Deletion of unlawfully processed data
<input type="checkbox"/>	An apology
<input type="checkbox"/>	Assurance that similar incidents will not occur in the future
<input type="checkbox"/>	Other (please specify):

Part 5: Declaration

I understand that the school/trust will investigate this complaint in accordance with its Data (Use and Access) Act 2025 Complaint Process.

Signature:

Date: