



The Olympus Academy Trust Privacy Notice – Parents and Learners

Document Summary

Document Owner:	Trust Data Protection Lead
Version:	7.0
Document Status:	Approved
Date Last Approved:	19 th June 2025
Date of Next Review:	19 th June 2027
Review Frequency:	2 Years
Owner: (Olympus or School)	Olympus Academy Trust
Governing Committee:	Audit & Risk Committee (ARC)
Statutory or Optional policy:	Optional
Appendices:	Appendix 1: Non-exhaustive list of the types of personal data we process. Appendix 2: Examples of whom we may share your data with where the law permits (non – exhaustive list) Appendix 3 – How Government uses your data
On Trust Website?	Yes
On School Websites?	Yes

Amendment History

Version	Amendment Date	Author	Amendment Summary
v3.1	18 th June 2020	Head of Business Operations	• New Trust document version system implemented. • Bi-annual review.
v3.1	6 th October 2020		• Approved by Audit & Risk Committee.
v3.1	15 th October 2020		• Approved by the Olympus Board of Trustees.
v4.0	15 th October 2020		• Policy issued.
v4.1	25 th February 2021	Head of Business Operations	• Update from Integra - policy amended to conform: • New paragraph added – 4.5 - 'collect and use learner information'. • New paragraph added – 7.2 - 'Youth Support Services (for learners aged 13+)' added. • New Section added – 9 – The Local Authority • New Section added – 13 – Connecting Care • New Section added – 14 – West Child Health Information System (CHIS)
v4.1	11 th March 2021		• Approved by Audit & Risk Committee.
v4.1	1 st April 2021		• Approved by the Board of Trustees
v5.0	1 st April 2021		• Policy Issued
v6.0	13 th April 23	Trust GDPR Lead	• Updates made to policy in line with new legislation following the introduction of the UK GDPR (changes made via tracked changes)
v6.1	4 th May 2023	Policy Coordinator	• Policy approved by Audit and Risk Committee
7.0	11 th June 2025	Trust Data Protection Lead	• Policy amended in line with new DPO, One West, template privacy notice

About this Privacy Notice

Individuals have a legal right to be informed about how we use their personal information. This Privacy Notice explains how we collect, store and use personal information. It is intended for learners and parents (including carers or guardians who we refer to in this privacy notice as 'parents') and we encourage all to read it. We also hold a separate Privacy Notice for the school's workforce and a shorter, simpler notice for learners themselves.

For the purposes of this privacy notice, 'the Trust' refers to all schools that are part of the Olympus Academy Trust.

Our aim is to always provide clear information about the personal information we are using and why we are using it. We have tried to keep the language in this Privacy Notice as simple as possible, however if anything is unclear or if you have any concerns, please contact gdpr@olympustrust.co.uk.

This Privacy Notice applies generally to the personal information that we collect and use. Unless there is a lawful reason not to do so, we will also provide more specific privacy information at the point at which we collect or use personal information, for example if we collect personal data via an online or paper form.

Whilst much of the personal information that we collect is mandatory (i.e. it must be provided so that we can manage the school, fulfil our legal obligations and provide an education), some of it is requested on a voluntary basis. We will explain to you whether there is a requirement to provide certain information to us, or whether you have a choice in doing so. Where this is the case, we will request consent at the point we collect the information.

For the purposes of data protection law, the Olympus Academy Trust (the Trust) is the 'Data Controller'. Our Data Protection Officer is One West; contact details are provided at the end of this privacy notice.

The personal data we hold (categories of personal data)

We process personal information to be able to run the school and Trust, to provide learners with an education and to make sure that we can look after our learners appropriately. We may collect information directly from learners or parents or from other places including other schools, the local council and the Department for Education (DfE). Examples of the types of personal data that we may collect, use, store and share (when appropriate) are listed at Appendix 1.

Our lawful reasons for processing learner/parent information (lawful bases)

Data Protection law requires us to have a legal reason ("Lawful Basis") for processing the personal data we use. These reasons are listed under Article 6 of the 'UK General Data Protection Regulation' (UK GDPR). Our lawful basis for processing will be explained at the point at which we collect personal information unless there is a lawful reason not to do so (for example where it is for the prevention or detection of crime).

The Trust processes a wide range of personal data for a variety of purposes, as described above. The lawful bases we rely on will therefore vary. However, generally, the lawful bases we mainly use in relation to learners and parents are:

- **We need to comply with the law (we have a legal obligation):** for example we collect and use learner information under legal and statutory obligations within the Education Act 1996, The Children Act 2004; Education and Inspections Act 2006; Education Act 2011; the Family and Children Act 2014 and Keeping Children Safe in Education (KCSIE).
- **We need to carry out a task in the public interest:** for example, the collection and use of learner information is necessary for us to perform our role as a school and to deliver our public task of providing education to our learners.

- **You have given us your consent** for example a photo of you for promotional purposes or our website.
- **We need to protect your vital interests (or someone else's interests)** this relates to life-or-death situations.
- **It is in ours or a third party's legitimate business interests to process the data** where this is the case, we will ensure that we have considered whether our legitimate interests are overridden by your rights and freedoms as the learner or parent.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so. We will then cease this aspect of processing.

When a learner is considered mentally capable of making their own decisions with regards consent (while there is no defined age, this is normally considered once a child attends secondary school), their consent choices over-ride those made by the parent or guardian.

Some of the reasons that we use for collecting and using information may overlap and there may be several grounds allowing us to use personal data. There are also other lawful bases that may apply, and this will be made clear wherever possible.

Our lawful basis for processing will be explained at the point at which we collect personal information unless there is a lawful reason not to do so (for example where it is for the prevention or detection of crime).

Special category (sensitive) personal information

We may also collect, store, and use information about you that falls into "special categories" of more sensitive personal data which has extra protection in law and requires us to identify a condition for processing under Article 9 of the UK GDPR.

Special category data is personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person (for example fingerprints)
- data concerning health; or
- data concerning a natural person's sex life or sexual orientation.

The Article 9 grounds which we may rely on to process special category data include:

- Legal obligation
- Substantial public interest including:
 - Statutory and government purposes
 - Equality of opportunity or treatment
 - Preventing and detecting unlawful acts
 - Preventing fraud
 - Public Health
 - Safeguarding

- Support for individuals with a particular disability or medical condition
- Explicit consent, for example to the use of biometric data, e.g. fingerprints.
- To maintain your vital interests

Further details about how the school complies with data protection legislation with regards the processing of Special Category data can be found in the Special Categories of Data section of the school's Data Protection Policy.

Criminal convictions

We may process data about criminal convictions or offences. This will usually be where such processing is necessary to carry out our obligations, to exercise our rights, to look after our learners and staff or to support the police and other relevant agencies.

We will only use information about criminal convictions or offences where the law allows us to. Usually this will either be based on our legal obligations in relation to safeguarding, preventing fraud, health and safety or with your consent. We also need to identify the relevant condition for the processing; this will usually be substantial public interest.

Collecting learner and parent information

The reasons that we collect and use personal information enable us to provide our learners with an education and to help us run the school. Please refer to **Appendix 1** for examples.

We collect and use information about you in a variety of ways including through the school application and admissions process, from correspondence with you and through assessing learners' educational progress. The ways in which we collect information about you may also include methods as outlined in **Appendix 1**.

We may also collect information about you from third parties such as information from other schools or other third parties engaging with you outside the school.

Whom we share learner information with

Information about learners and parents will not be shared with any third party without consent, unless the law allows us to do so. Where it is legally required or necessary (and it complies with data protection law), personal information may be shared with the relevant local authority to meet our legal obligations to share information such as safeguarding concerns, or we are legally obligated to share certain data with the Department for Education (DfE). To find out more about the data collection requirements that are placed upon us by the DfE including the data that we share with them go to: <https://www.gov.uk/education/data-collection-and-censuses-for-schools>. We do not use data for profiling, and only for marketing if you have opted in.

If you leave us and move to an alternative school, we are legally obligated to transfer your child's Education Record and all Safeguarding files onto the new school, to ensure their education and any additional support is in no way compromised by the move.

In the course of investigations, complaints or incidents (such as safeguarding incidents), we may need to disclose information to third parties in order to establish the facts of a case, explain our decisions and ensure transparency in our processes.

Further examples of with whom we share data are listed at **Appendix 2**. Details of how we share data with the Department for Education can be seen in **Appendix 3**.

Third-Party Processors

There are occasions when we contract or commission third party organisations or software

systems to carry out functions on our behalf, and inevitably these functions will involve those third parties processing personal data on our behalf.

Third-Party Processors are acting on our behalf, and under our instruction are governed by a contract that meets the requirements defined by GDPR.

Youth support services [For use by educational settings with learners aged 13+:]

Learners aged 13+

Once our learners reach the age of 13, we also pass learner information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the learner once they reach the age 16.

Data is securely transferred to the youth support service via email and is held for the relevant retention period.

Learners aged 16+ [For use by educational settings with learners aged 16+:]

We will also share certain information about learners aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

A child / learner, once they reach the age of 16, can object to only their name, address and date of birth is passed to their local authority or provider of youth support services by informing us.

Data is securely transferred to the youth support service via email and is held for the relevant retention period.

For more information about services for young people, please visit our local authority website.

Storing learner and parent data

Personal data is stored in line with our data protection policy in a range of different places, including within learners' files and our IT systems, and the school's email system.

The information that we create and maintain is kept secure. Once a learner's education with us has ended, we may retain such information beyond their attendance at the school as deemed necessary and in line with our retention policies. A copy of the Retention Schedule can be obtained by contacting gdpr@olympustrust.co.uk.

Transferring data internationally

Where we transfer personal data to a country or territory outside the UK and European Economic Area, we will do so in accordance with data protection law and ensure that we have sufficient safeguards in place.

Requesting access to your personal data

Individuals have the right to request access to information about them that we hold. This is known as making a 'Subject Access Request' (SAR). If you make a subject access request and we hold information about you, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- Give you a copy of the information in an intelligible form within a month unless an extension is necessary on the ground of the complexity of the request.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request, please contact gdpr@olympustrust.co.uk.

Children have the same rights as adults over their personal data and the Trust will assess each request on its own merits. Learners can find out what personal information we hold about them and how we use it by making a subject access request, as long we judge that they can properly understand their rights and what this means.

Those with parental responsibility can make a request with respect to their child's data, where the child is not considered mature enough to understand their rights over their own data (mental capacity will be judged by the school on a case-by-case basis), or where the child has provided consent and it is considered to be in the best interests of the child. Parents also have the right to make a subject access request with respect to the personal data the school holds about themselves. If you would like to make such a request, please contact gdpr@olympustrust.co.uk.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Request to have personal data corrected if you believe that it is inaccurate or incomplete.
- Request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Restrict our processing of personal data (i.e. permitting its storage but no further processing) under certain circumstances.
- Object to processing if we are processing your information as part of our public tasks, or on the basis of our legitimate business interests, in which case we will consider your objection, and balance this against our need to process the information.
- Object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics.
- Withdraw your consent to processing.

- Have personal information, which you have provided, transmitted electronically to another organisation in certain circumstances.
- Not be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect unless you have agreed or in other limited circumstances.
- Seek redress, either through the ICO, or through the courts.

Contact and Complaints

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please either contact gdpr@olympustrust.co.uk.

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please contact the Trust Data Protection Lead (gdpr@olympustrust.co.uk) or our Data Protection Officer One West: i-west@bathnes.gov.uk or 01225 395959.

You can also complain to the Information Commissioner's Office if you are unhappy with how we have used your data, but they would generally expect you to have raised the issue with us first:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>

Links to other policies:

- Data Protection Policy
- Freedom of Information
- CCTV Policy
- Records Retention Policy
- Online Safety Policy
- All other Privacy Notices

Diversity, Equity, and Inclusion Statement

We are committed to fostering a diverse, equitable, and inclusive environment where every individual is valued and respected. Our policies reflect our dedication to creating a workplace that embraces differences and promotes fairness. We believe that diversity enriches our organisation and drives innovation, and we strive to ensure that all employees have equal opportunities to succeed and thrive.

Appendix 1: Non-exhaustive list of the types of personal data we process.

Data type	Purpose	Where we obtain the data from
Personal identifiers and contacts (such as name, unique learner number, contact details and address).	To contact parents/carers, support learning, manage enrolment and ensure safety	School application from the local authority, direct from the parent or learner, CTF files from the previous school
Characteristics (such as ethnicity, language, and free school meal eligibility).	To monitor equality and diversity, report to the Government and support learner needs	Direct from the parent or learner, school application forms.
Safeguarding information (such as court orders and professional involvement).	To protect learner welfare and comply with safeguarding duties	Local authority, social services, previous schools, direct from parents
Special educational needs (including the needs and ranking).	To provide appropriate support and resources, and meet statutory obligations	Direct from the parent or learner, previous schools, education psychologists, SEN assessments
Medical conditions (such as doctor information, child health, dental health, allergies, medication, and dietary requirements).	To ensure learner health and safety, manage medical needs, and respond to emergencies	Direct from the parent or learner, healthcare professionals
Attendance record (such as sessions attended, number of absences, absence reasons and any previous schools attended).	To monitor attendance, identify patterns and report to authorities	School registers, previous schools
Test results, assessment, and attainment (e.g. KS2 SATs, GCSEs, A Levels, and any other relevant results)	To track academic progress, tailor teaching, and report to parents and authorities	Internal assessments, previous schools, national testing bodies
Behavioural information (such as exclusions and any relevant alternative provision put in place).	To manage behaviour, provide support, and ensure a safe learning environment	Internal school records, previous schools.
Photographs and CCTV	To promote the school, ensure safety and support behaviour management	Taken by the school
Biometric data (such as fingerprints)	To manage access to cashless catering	Collected directly from the learner with consent
We may use online platforms to deliver lessons remotely; if we intend to record the lesson, we will let you know	To support learning and provide access to missed lessons	Recorded during online lessons with prior notice.

Appendix 2: Examples of whom we may share your data with where the law permits (non – exhaustive list)

- The Local Authority (South Gloucestershire Council).
- Schools that learners attend after leaving.
- The Department for Education (DfE).
- The National Health Service to support learner safety and vaccination programs.
- The learner's family and representatives.
- Educators and examining bodies.
- The schools' inspector
- Suppliers and service providers so that they can provide a contracted service such as careers and Physical Education provision.
- Central and local government.
- Auditors.
- Survey and research organisations.
- Security organisations.
- Health and social welfare organisations.
- Professional advisers and consultants.
- Counsellors/Educational Psychologists as and when appropriate.
- Charities and voluntary organisations.
- Police forces, courts, tribunals.
- Professional bodies.
- Our Data Protection Officer on occasion, e.g. to support a subject access request.
- Occasionally with school governors and trustees.

We may be required to share information about our learners with the local authority to ensure that they can conduct their statutory duties under the Schools Admission Code, including conducting Fair Access Panels.

Appendix 3 – How Government uses your data.

The learner data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school).

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example, via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities, and awarding bodies. To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools.
- local authorities.
- researchers.
- organisations connected with promoting the education or wellbeing of children in England.
- other government departments and agencies.
- organisations fighting or identifying crime.

Appendix 4: Third Party Processors we use.

Third Party Processor	Personal data captured	Purpose	Country the data is processed in	Who the information may be shared with and why
Wonde	Learner personal information including name, date of birth, contact details, attendance data, demographic information (such as nationality, ethnicity and religion where held), medical information relevant to education, and Free School Meal eligibility.	Provides secure data integration between the school's Management Information System (MIS) and approved educational applications, ensuring data is kept up to date and enabling secure statutory and operational data sharing.	UK	Approved educational software providers authorised by the school, the Local Authority and the Department for Education where required for statutory purposes, using secure data transfer.
Arbor	Personal information relating to learners, parents/carers, guardians, and staff, including names, contact details, addresses, attendance, behaviour, assessment, curriculum, safeguarding, SEND and educational records.	Provides the school's Management Information System (MIS) to support learner and staff administration, teaching and learning, safeguarding, statutory reporting, attendance, assessment, communication and operational management.	UK	Authorised school staff, parents/carers, the Department for Education, the Local Authority, examination boards, education and safeguarding partners, healthcare professionals where appropriate, other educational establishments where learners transfer, Arbor Education as the system provider, and approved third-party systems integrated with Arbor. Information is shared only where necessary to support education, safeguarding, statutory reporting and the school's legal obligations.
CCTV	CCTV images and video recordings of learners, staff, visitors and contractors; date and time stamps; vehicle registration numbers (where applicable); camera location; and audit logs relating to authorised system users.	To protect the safety and welfare of learners, staff and visitors; support safeguarding; prevent and detect crime, vandalism and anti-social behaviour; secure school premises; investigate incidents and complaints; and support health and safety.	UK	Authorised school staff (e.g. Headteacher, senior Authorised school staff (including senior leaders, the Site Manager and the Designated Safeguarding Lead where appropriate), the Police, the Local Authority, insurers, legal representatives and other statutory agencies where necessary to investigate incidents or comply with legal obligations. The school's CCTV maintenance provider may also access the system for support under a data processing agreement. Information is shared only where necessary and lawful.

