Policy Name:	DATA PROTECTION POLICY
Policy Type	Statutory
Issue Date	19th May 2024
To Be Reviewed	Annually: 19th May 2025
Approved by Governing Body	Trust Board

This policy was drafted in accordance with the requirements of the General Data Protection Regulation (GDPR) WEF 25 May 2018.

1. Policy Statement

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as a trust we will collect, store and process personal data about our students, staff, parents/carers and others. This makes us a data controller in relation to that personal data.

We are committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our staff at Orbis Education Trust must, therefore, comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

All staff at Orbis Education Trust involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities through an ongoing programme of staff training.

2. About this Policy

The types of personal data that we may be required to handle include information about students, parents/carers, our staff and others that we have dealings with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other regulations (together 'Data Protection Legislation').

This policy, and any other documents referred to in it, sets out the basis upon which we will process any personal data that we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.

3. Definition of Data Protection Terms

Data Protection Officer

As a trust we are required to appoint a Data Protection Officer (DPO). Our DPO is **Mr Christopher Roberts, Orbis Executive Director responsible for compliance** and can be contacted at dpo@Orbismat.com. The DPO is responsible for ensuring compliance with data protection legislation and this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO. The DPO is, also, the central point of contact for all data subjects and others in relation to matters of data protection.

Data Protection Principles

Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

- processed fairly, lawfully and transparently in relation to the data subject;
- processed for specified, lawful purposes and in a way which is not incompatible with those purposes;
- adequate, relevant and not excessive for the purpose;
- accurate and up to date;
- not kept for any longer than is necessary for the purpose;
- processed securely using appropriate technical and organisational measures.

Personal data must also:

- be processed in line with data subjects' rights;
- not be transferred to people or organisations situated in other countries without adequate protection.

We will comply with these principles in relation to any processing of personal data by the trust.

Fair and Lawful Processing

Data protection legislation is not intended to prevent the processing of personal data, rather it is to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed fairly, data subjects must be made aware:

- that the personal data is being processed;
- why the personal data is being processed;
- what the lawful basis is for that processing;
- whether the personal data will be shared and, if so, with whom;
- of the period for which the personal data will be held;
- of the existence of the data subject's rights in relation to the processing of that personal data;
- of the right of the data subject to raise a complaint with the Information Commissioner's Office (ICO) in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing.

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the data protection legislation. We will normally process personal data under the following legal grounds:

- where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;
- where the processing is necessary to comply with a legal obligation that we are subject to (e.g. the Education Act, 2011);
- where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest; and
- where none of the above apply, we will seek the consent of the data subject to the processing of their personal data.

When special category personal data is being processed, an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

- where the processing is necessary for employment law purposes, for example in relation to sickness absence;
- where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the processing is necessary for health or social care purposes, for example in relation to students with medical conditions or disabilities; and
- where none of the above apply, we will seek the consent of the data subject to the processing of their special category personal data.

We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a student joins us.

If any data user is in doubt as to whether they can use any personal data for any purpose, then they must contact the DPO before doing so.

Vital Interests

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

Where none of the other bases for processing set out above apply then the trust must seek the consent of the data subject before processing any personal data for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

When students and/or staff join the trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate, third parties may, also, be required to complete a consent form.

In relation to our students in Years 7 to 11, we will seek consent from an individual with parental responsibility for that student.

When students enter our sixth form, we will generally seek consent directly from the student themselves, however, we recognise that this may not be appropriate in certain circumstances and, therefore, may be required to seek consent from and individual with parental responsibility.

If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

- inform the data subject of exactly what we intend to do with their personal data;
- require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- inform the data subject of how they can withdraw their consent.

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

The DPO must always be consulted in relation to the creation of new or amendment to existing consent collection forms before they are issued.

A record must always be kept of any consent, including how it was obtained and when.

Processing for Limited Purposes

In the course of our activities as a trust, we may collect and process the personal data set out in our privacy statements. This may include personal data that we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data that we receive from other sources (including, for example, local authorities, other schools, parents/carers, other students or members of our staff).

We will only process personal data for the specific purposes set out in our Privacy Statements or for any other purposes specifically permitted by data protection legislation or for which specific consent has been provided by the data subject.

Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them about:

- our identity and contact details as Data Controller and DPO;
- the purpose or purposes and legal basis for which we intend to process that personal data;
- the types of third parties, if any, with which we will share or to which we will disclose that personal data;
- whether the personal data will be transferred outside the European Economic Area (EEA) and, if so, the safeguards in place;
- the period for which their personal data will be stored, by reference to our Retention and Destruction Policy;
- the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and
- the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible thereafter, informing them of where the personal data was obtained from.

Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by data protection legislation.

Accurate Data

We will ensure that personal data we hold is accurate and kept up to date.

We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Data subjects have a right to have any inaccurate personal data rectified. See further below in relation to the exercise of this right.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required as directed by the Orbis Data Retention and Destruction Guidance.

Processing in Line with Data Subjects' Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- request access to any personal data we hold about them;
- object to the processing of their personal data, including the right to object to direct marketing;
- have inaccurate or incomplete personal data about them rectified;
- restrict processing of their personal data;
- have personal data we hold about them erased;
- have their personal data transferred; and
- object to the making of decisions about them by automated means.

The Right of Access to Personal Data

Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the trust's Subject Access Request (SAR) Procedure.

The Right to Object

In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing investigations that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

An objection to processing does not have to be complied with where the trust can demonstrate compelling legitimate grounds which override the rights of the data subject.

Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

In respect of direct marketing any objection to processing must be complied with.

The trust is not, however, obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

The Right to Rectification

If a data subject informs the trust that personal data held about them by the trust is inaccurate or incomplete, then we will consider that request and provide a response within one month.

If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case.

We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the ICO at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

Data subjects have a right to 'block' or suppress the processing of personal data. This means that the trust can continue to hold the personal data but not do anything else with it.

The trust must restrict the processing of personal data:

- where it is in the process of considering a request for personal data to be rectified;
- where the trust is in the process of considering an objection to processing by a data subject;
- where the processing is unlawful but the data subject has asked the trust not to delete the personal data; and
- where the trust no longer needs the personal data but the data subject has asked the trust not to delete the personal data because they need it in relation to a legal claim, including any potential claim against the trust.

If the trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

Data subjects have a right to have personal data about them held by the trust erased only in the following circumstances:

- where the personal data is no longer necessary for the purpose for which it was originally collected;
- when a data subject withdraws consent – which will apply only where the trust is relying on the individual's consent to the processing in the first place;
- when a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see above in relation to the right to object;
- where the processing of the personal data is otherwise unlawful;
- when it is necessary to erase the personal data to comply with a legal obligation.

The trust is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- to exercise the right of freedom of expression or information;
- to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
- for public health purposes in the public interest;
- for archiving purposes in the public interest, research or statistical purposes; or
- in relation to a legal claim.

If the trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

The DPO must be consulted in relation to requests under this right.

Right to Data Portability

In limited circumstances a data subject has a right to receive their personal data in a machine readable format, and to have this transferred to other organisation.

If such a request is made, then the DPO must be consulted.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Security procedures include:

- **Entry controls**. Any stranger seen in entry-controlled areas should be reported to the main reception.
- **Secure lockable desks, cupboards and filing cabinets**. Desks, cupboards and filing cabinets should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).
- **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the ICO's guidance on the disposal of IT assets.
- **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when left unattended.
- **Working away from trust premises – paper documents**. Wherever possible paper documents should not be taken offsite. If this is unavoidable they should be locked in a secure location at all times.
- **Working away from trust premises – electronic working**. Staff should log into our secure network if working away from the site. Portable data devices such as USBs, etc. may only be used if they have been encrypted. All existing devices need to be encrypted by IT services. Upon termination of contract, staff should delete data from all such devices.
- **Document printing**. Documents containing personal data must be collected immediately from printers and not left on photocopiers.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

Data Protection Impact Assessments

The trust takes data protection very seriously and will consider and comply with the requirements of data protection legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

The trust will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.

The DPO should always be consulted as to whether a data protection impact assessment is required and if so how to undertake that assessment.

Disclosure and Sharing of Personal Information

We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools and other organisations where we have a lawful basis for doing so.

The trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

In some circumstances we will not share safeguarding information. Please refer to our Safeguarding Policy.

Further detail is provided in our Privacy Statements.

Data Processors

We contract with various organisations who provide services to the trust, whose details are listed in our Privacy Notices.

In order that these services can be provided effectively we are required to transfer personal data of data subjects to these data processors.

Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the trust. The trust will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

Contracts with data processors will comply with data protection legislation and contain explicit obligations on the data processor to ensure compliance with the data protection legislation, and compliance with the rights of data subjects.

Images and Videos

Parents/carers and others attending trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents/carers can take video recordings of a trust performance involving their child. The trust does not prohibit this as a matter of policy.

The trust does not, however, agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the trust to prevent.

The trust asks that parents/carers and others do not post any images or videos which include any child other than their own on any social media or otherwise publish those images or videos.

As a trust we want to celebrate the achievements of our students and, therefore, may want to use images and videos of our students within promotional materials or for publication in the media, such as local, or even national, newspapers covering trust events or achievements. We will seek the consent of students, and their parents/carers where appropriate, before allowing the use of images or videos of students for such purposes.

Whenever a student begins their attendance at the trust they, or their parent/carer, where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that student. We will not use images or videos of students for any purpose where we do not have consent.

Biometric Recognition Systems

Where we use student's biometric data as part of an automated biometric recognition system (for example, students use finger prints to purchase food instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric systems. We will provide alternative means of accessing the relevant services for those students.

Parents/carers and students can object to participation in the school's biometric recognition systems, or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parents/carers.

Where staff members or other adults use the school's biometric systems, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

Use of Digital Staff Images

Orbis Education Trust recognises its responsibilities with regard to the confidential personal data of its employees and this, also, applies to digital images of staff.

The following outlines the trust policy with regard to still and video images taken of staff:

- All staff will have a photograph taken when they are employed at Orbis Education Trust in order to produce their identity badge. This image will, also, be displayed on Arbor and will appear when sending emails internally. It will, also, be used for photo boards within the

trust so that students get to recognise staff and their roles and responsibilities. This is seen as appropriate action to safeguard the students and staff on site.

- During the course of the year, other photos may be taken, or video footage shot which may be used for promotional purposes or for websites (e.g. a photo of the staff quiz team to be put on the website, or a video clip which may be included in an open evening speech and put on a website).

CCTV

The trust operates a CCTV system. Please refer to the CCTV Policy.

Changes to this policy

We may change this policy at any time. Where appropriate, we will notify data subjects of those changes.