OMNIA
FOUNDATION

DATA PROTECTION POLICY

Policy type	Omnia Foundation
Review period	Annual
Last reviewed on	Spring 2024
Next review due	Spring 2025
Approval level	Executive Board

Approved by (Name, date, signature)

Chair of Executive Board, 15 February 2024
Chair of Executive Board, David Kreyling
Published on Omnia Foundation Website (staff area)

OMNIA
FOUNDATION

POLICY FOR DATA PROTECTION

Mission

We believe in investing in people. As professionals in the teaching and training professions, we strive to provide a better future for the children, young people and home settings we work with. Success for us means unleashing the potential of each individual so they can grow, develop and reach the potential of which they are capable. Our values are grounded in our determination to be the change we want to see in the world, through passion, commitment and integrity. We strive to plant a seed of kindness and compassion in a generation that will produce resilience and hope and enable them to aspire and achieve productive and fulfilled lives. Our success is measured in the lives we changed.

At the Omnia Foundation, we create a secure and safe environment that encourages communication, self-belief, mutual respect and success. We provide a rich and balanced curriculum that develops every child, allowing them to achieve their true potential.

Aims of the policy

This policy aims

- To ensure that all personal data collected about staff, students, adults in the home setting, board members, visitors and other individuals is collected, stored and processed in accordance with UK data protection law
- To outline clearly the processes and procedures in place to minimise the risk to personal data
- To ensure that all staff, students, adults in the home setting, board members, visitors and other individuals fully understand that personal data is sensitive and should be treated with due care and attention
- To ensure that all staff, students, adults in the home setting, board members, visitors and other individuals fully understand the measures put in place by the foundation to minimise the risk to personal data
- To set out how the foundation intends to comply with the principles of data protection

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

This policy should be read in conjunction with the Data Record Management and Retention Policy, the Data Breach Policy, the Subject Access Request Policy, the Protection of Biometric Information of Students Policy and all related privacy notices.

Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

> Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Safeguarding information • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The data controller

The Omnia Foundation processes personal data relating to students, their home settings, staff, Executive Board members, visitors and others, and therefore is a data controller.

The foundation is registered with the ICO / has paid its data protection fee to the ICO, as legally required. (Delete as applicable.)

OMNIA FOUNDATION

Roles and responsibilities

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

Executive Board

The Executive Board has overall responsibility for ensuring that the foundation complies with all relevant data protection obligations.

Chief Operating Officer

The Chief Operating Officer, on behalf of the Executive Board, is responsible with the Data Protection Officer to ensure that the foundation complies with all relevant data protection obligations.

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 Executive Board and, where relevant, report to the board their advice and recommendations on data protection issues across the foundation.

The DPO is also the first point of contact for individuals whose data is processed by the foundation, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Fiona Grocock and is contactable via email at fiona.grocock@centralserviceslimited.co.uk

Head of Foundation

The Head of Foundation acts as the representative of the data controller on a day-to-day basis

All staff

Staff are responsible for:

> Collecting, storing and processing any personal data in accordance with this policy

> Informing the foundation of any changes to their personal data, such as a change of address

> Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

OMNIA FOUNDATION

Data protection principles

The UK GDPR is based on data protection principles with which the Omnia Foundation must comply.

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

Collecting personal data

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 foundation can fulfil a contract with the individual, or the individual has asked the foundation to take specific steps before entering into a contract

> The data needs to be processed so that the foundation can comply with a legal obligation

> The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life

> The data needs to be processed so that the foundation can perform a task in the public interest or exercise its official authority

> The data needs to be processed for the legitimate interests of the foundation(where the processing is not for any tasks the foundation performs in the public interest) or a third party, provided the individual's rights and freedoms are not overridden

> The individual (or an adult from their home setting when appropriate in the case of a student) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

> The individual (or a adult from their home setting when appropriate in the case of a student) has given explicit consent

> The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law

> The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent

> The data has already been made manifestly public by the individual

> The data needs to be processed for the establishment, exercise or defence of legal claims

> The data needs to be processed for reasons of substantial public interest as defined in legislation

> The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

> The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

> The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

> The individual (or a adult from their home setting when appropriate in the case of a student) has given consent

> The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent

> The data has already been made manifestly public by the individual

> The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights

> The data needs to be processed for reasons of substantial public interest as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 foundation's record retention schedule (please refer to the Data Records Management and Retention Policy.

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

> There is an issue with a student or adult from the home setting that puts the safety of our staff at risk

> We need to liaise with other agencies – we will seek consent as necessary before doing this

> Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 students or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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

> Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing

> The right to lodge a complaint with the ICO or another supervisory authority

> 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

> The safeguards provided if the data is being transferred internationally

For further details on how to make a subject access request, please refer to the Subject Access Request Policy.

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

Children and subject access requests

Personal data about a child belongs to that child, and not adults from the child's home settting. For an adult from the student's home setting 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 adults from the home settings of students at the foundation may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

> Withdraw their consent to processing at any time

> Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)

> Prevent use of their personal data for direct marketing

> Object to processing which has been justified on the basis of public interest, official authority or legitimate interests

> Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

> 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.

Parental requests to see the educational record

Since the Omnia Foundation is an independent school, there is no automatic parental right of access to the educational record of their child.

However, in view of the fact that all our students are subject to an Education, Health and Care Plan, we will consider subject access requests in certain circumstances and where releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

Please see the Subject Access Request Policy for more details.

Photographs and videos

As part of our programme of activities, we may take photographs and record images of individuals within the foundation.

We will obtain written consent from adults in the home setting for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the home setting and student.

Any photographs and videos taken by adults from the home setting at foundation events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant adults from the other student's home setting have agreed to this.

Where the foundation takes photographs and videos, uses may include:

> Within the foundation site on notice boards and in foundation brochures, newsletters, etc.

> Outside of the foundation by external agencies such as newspapers and media campaigns

> Online on the foundation website or social media pages. Please refer to the Facebook Page Policy for further information on how this data is managed.

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.

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 processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law

> Completing data protection impact assessments where the foundation's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

> Integrating data protection into internal documents including this policy, any related policies and privacy notices

> Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

> Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

> Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply

> Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of the foundation 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

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, 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 foundation office

> Passwords that are at least 10 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff and students are reminded that they should not reuse passwords from other sites

> Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

> Staff, students or executive board members who store personal information on their personal devices are expected to follow the same security procedures as for foundation-owned equipment

> 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

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 foundation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The Omnia Foundation 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 the Data Breach Policy.

Training

All staff and executive board members are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the foundation's processes make it necessary.

Monitoring and review

The Chief Operating Officer and the DPO will monitor this policy periodically and review it annually.

The annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies.