Data Protection Policy

Responsible:	School Business Manager/Data Protection Officer
Responsible Committee:	Finance, Audit & Premises Committee
Implementation Date:	July 2023
Date of Review:	July 2023
Date of Next Review:	June 2026

Any Associated Policies:	None

Introduction

Global Academy needs to keep certain information about students, staff, governors and other stakeholders to deliver teaching and learning, monitor student progress, performance, achievements, and ensure the health and safety of staff and students. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. In line with article 5 of the General Data Protection Regulation (GDPR), the Academy will comply with the following data protection principles and will ensure that personal information is:

- Processed in a lawful, fair and transparent manner;
- Collected for a specified and legitimate purpose – and not processed in a manner which is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- Processed in a manner that ensures appropriate security of the personal data.

Global Academy staff and others who process or use any personal information must ensure that they follow these principles at all times.

Notification of Data Held and Processed

All staff, students, governors and other users are entitled to know:

- what information the Academy holds and processes about them and why;
- how to gain access to it;
- how to keep it up to date;
- what the Academy is doing to comply with its obligations under GDPR.

The Academy will ensure that staff data is updated as and when necessary. Students' data is updated annually through the enrolment process and as necessary due to individual circumstances.

Responsibilities of Staff

All staff are responsible for maintaining their personal data held by the Academy.

All staff are responsible for checking that any information that they provide to the Academy in connection with their employment is accurate and up to date. Staff must also inform the Academy of any errors or changes e.g. changes of address or contact numbers. The Academy cannot be held responsible for any errors unless the staff member has informed the Academy of them.

If and when, as part of their responsibilities, staff collect information about other people, (e.g. students), they must comply with the Academy's procedures and guidance.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Personal information should be:

- kept on the Academy network including OneDrives, and not stored on hard drives of PCs, laptops or other devices including memory sticks, or personnel devices
- kept in a locked filing cabinet, or
- in a locked drawer, or
- in a private office, or
- if it is electronic, be password-protected.

Computers where personal data can be accessed must be logged off or locked (password enabled) when the user is not in attendance.

Staff should note that Data Protection compliance is ultimately the responsibility of all staff. Individuals can be held legally responsible if they disclose personal information to any unauthorised third party. Breaches of data protection rules are considered to be a disciplinary matter and may be considered gross misconduct in some cases.

In the event of an actual or a suspected data breach, staff should follow the procedure in Appendix 1.

Data Sharing

The Academy only shares personal data with organisations who have implemented data protection policies in line with GDPR guidance. The Academy outlines its processes for data sharing in its privacy notice (Appendix 2) which includes the sharing of data for child protection purposes.

Where the Academy uses proprietary software subscriptions to process personal data on its behalf, it requires them to do so on the basis of written instructions, be under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Student Obligations

Students must ensure that all personal data provided to the Academy is accurate and up to date. They must ensure that changes of address, etc., are reported to the reception.

If students using the network process any personal data, they must ensure that they comply with the Academy's policy and the requirements of GDPR.

The Lawful Basis on which we use this Information

The Academy collects personal data under GDPR Article 6c (Legal Obligation), and 6e (Public Task) in order to meet its legal obligations with the ESFA. This is also necessary in order to carry out the public task to provide education and training. Details on the categories of data collected and who this is shared with can be found in the privacy notice (Appendix 2).

Retention of Data

Information about students will be retained for a maximum of six years after they leave so that a reference can be provided or to confirm enrolment status for other reasons. As such, references cannot be provided for students who have left more than six years ago.

The Academy will retain staff applicant data for six months after the application process has finished so that it can effectively deal with re-applications.

Information about staff will be retained for the duration of their employment and for six years after they leave the Academy.

Examination Marks

Students will be entitled to information about their marks for both coursework and non-examination assessments. In line with the retention policy, past examination information will be available for six years after students leave.

Rights to Access Information

Students, parents, staff and governors have the right to access any personal data that is kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the "Subject Access Request" form and submit it to the Academy's Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request.)

The Academy may charge a fee if the request is manifestly unfounded or excessive.

The Academy aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

The Right to be Forgotten

Students, parents, staff and governors have the right to obtain the erasure of personal data where this data is no longer necessary in relation to the purposes for which they were collected and processed.

However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

Any person who wishes to exercise this right should complete the "Subject Access Request" form and submit it to the Data Protection Officer. (Completion of this form is not mandatory but doing so will accelerate a request)

The Academy may charge a fee if the request is manifestly unfounded or excessive.

The Academy aims to comply with requests as quickly as possible but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

The Data Controller and the Designated Data Controller(s)

The Academy is the Data Controller under GDPR, and the Board of Governors is ultimately responsible for implementation of this policy. However, the designated Data Protection Officer will deal with day-to-day matters.

Public Register of Data Controllers and Notification

The Academy has a valid notification in the data protection register that relates to processing information. This can be viewed at https://ico.org.uk. It is the responsibility of the Data Protection Officer to ensure the registration is checked and updated on a regular basis.

Registration Number: ZA186086

Data Controller: The Global Academy UTC Trust Ltd

Data Protection Officer

The nominated Data Protection Officer at Global Academy is:

Beth Holmes
DPO@globalacademy.com

The Global Academy
Blyth Road
Hayes
Middlesex
UB3 1HA

Conclusion

Compliance with GDPR is the responsibility of all members of the Academy. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to Academy facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Protection Officer.

Privacy Notice

Under data protection law, individuals have a right to be informed about how the Academy uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals when we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about students. Global Academy is the 'data controller' for the purposes of data protection law.

The personal data we hold about you:

- Your full name
- Your home address
- Your contact number(s)
- Your email address

If at any time you need to advise as us of a change in your personal data, you can make a request verbally or in writing.

The personal data we hold about your child:

Personal data that we may collect, use, store and share (when appropriate) about students includes, but is not restricted to:

- Contact details, date of birth, identification documents.
- Results of internal assessments and externally set tests
- Student and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about students that we have received from other organisations, including other schools, local authorities and the Department for Education.

Examples on why we use your child's data

We use this data to:

- Support student learning
- Monitor and report on student progress
- Provide appropriate pastoral care
- Protect student welfare
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use students' personal data to comply with a legal obligation or to perform an official task in the public interest.

Where we have obtained consent to use students' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Collecting this information

While the majority of information we collect about students is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

Data sharing

We do not share information about students with any third party without consent unless the law and our policies allow us to do so. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Storage and security

Personal data is held according to our GDPR policy, which is accessible via our school website, and in compliance to the UK GDPR regulations.

Parents and students' rights regarding personal data

You have the right to make a **'subject access request'** to gain access to personal information that the school holds. Parents/carers 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 (usually under the age of 12), or where the child has provided consent. We will respond in a timely manner. However, we may find it difficult to respond in the school holidays.

Other rights

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

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer DPO@globalacademy.com

Subject Access Request

Recital 63 of the General Data Protection Regulations (GDPR) states *a data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.* Data subjects are also able to request the erasure of their data if it is no longer necessary in relation to the purposes for which it was collected and processed. However, there are certain limits on this right, such as the need to retain data for funding or safeguarding and obligations.

You can request to access your data via phone, email or verbally. However, in order to process your request as quickly and efficiently as possible we would ask that you complete this form. You will also need to provide proof of identity, usually this would be by communicating via an email address that the school already has on file for you. However, if this cannot be done, proof of identity (such as a birth certificate, passport, driving licence or an official letter addressed to you at your home address) would need to be provided. Your request will be processed within 30 calendar days on receipt of a completed form and proof of identity.

Global Academy generally does not charge for subject access requests but it may charge a fee if the request is manifestly unfounded or excessive.

Please provide the below information and return this form to:
DPO@globalacademy.com
Global Academy,
The Old Vinyl Factory,
1 Record Walk,
Hayes,
Middlesex,
UB3 1DH

Personal Information

Title:

Surname:

First Name(s):

Date of Birth:

Address:

Previous Address (Known to the Academy):

Telephone number:

Please outline below the details of your request.

Are you requesting the erasure of your data?

Yes ☐ **No** ☐

Please tick the box below that is relevant to the data held by the Academy:

Employment Information ☐

Student Information ☐

Please provide the dates you attended/were employed by the Academy. Please also provide your learner/employee number if possible.

Declaration:

I confirm that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that Global Academy is obliged to confirm proof of identity and it may be necessary to obtain further information in order to comply with this subject access request.

Name

Signature

Date

Data Breach Notification Procedure

Global Academy holds, processes and shares a large amount of personal data. Every care is taken to protect personal data and avoid a data protection breach that could compromise security.

The Scope of this Procedure

This procedure relates to all personal and sensitive data held by the Academy, regardless of format. The procedure applies to all staff and students at the Academy, including contractors, consultants, suppliers and data processors working for, or on behalf of the Academy.

The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Types of Breach

For the purpose of this procedure, data security breaches include both confirmed and suspected incidents. An incident, in the context of this procedure, is an event or action, which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes, but is not restricted to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (for example loss of a laptop, tablet device, mobile phone or paper record).
- Unauthorised use of, access to or modification of data or information systems.
- Attempts to gain unauthorised access to information or IT systems, regardless of whether these attempts were failed or successful.
- Unauthorised disclosure of sensitive or confidential data.
- Unforeseen circumstances such as a fire or flood.
- Other human error.

Responding to Personal Data Breaches

All Academy staff must report any actual or possible data breach immediately (within 12 hours of becoming aware of the breach) to the Data Protection Officer by emailing DPO@globalacademy.com

The report will include full and accurate details of the incident, when the breach occurred, who is reporting it, the nature of the information and how many individuals were involved.

Containment and Recovery

The Data Protection Officer will determine if the breach is still occurring and, if so, the appropriate steps will be taken to immediately minimise the effect of the breach.

The steps taken by the Data Protection Officer when responding to a personal data breach may include:

- Ensuring that the personal data breach is contained as soon as possible.
- Assessing the level of risk to data subjects as soon as possible.
- Gathering and collating information from relevant sources.
- Informing all interested persons within the Academy of the personal data breach and the investigation.
- Assessing the level of risk to the Academy.
- Notifying supervisory authorities (with 72 hours), data controllers, data subjects and others of the breach in accordance with this procedure.

The Data Protection Officer is primarily responsible for investigating possible or actual personal data breaches and for determining whether any notification obligations apply. The investigation will need to take into account the following:

- The type of data involved and its sensitivity
- The protections that are in place
- What has happened to the data (for example if it has been lost or stolen)
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, the number of individuals involved and the potential effect on those data subjects.
- Whether there are wider consequences to the breach.

All staff must cooperate with the Data Protection Officer in relation to the investigation and notification of personal data breaches.

Notification

The Data Protection Officer is responsible for determining who needs to be notified of the breach and every incident will be assessed on a case-by-case basis.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Information on what action has already been taken to mitigate risks should also be shared along with advice on what the individuals can do to protect themselves further. Individuals should also be provided with a way to contact the Academy if they have any further concerns or questions about the breach.

If a large number of people are affected or there are serious consequences the Information Commissioner's Office (ICO) should be notified.

The Data Protection Officer will keep a full record of the breach, including the details of the breach, its effects and the remedial action taken.

Evaluation

Once the initial incident is contained the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the responses and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy and whether any further action is needed to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and stored.
- Where the biggest risks lie and whether there are any concerns regarding existing measures.
- Staff awareness.