

Data Protection Policy

Effective Date: 21 09 2023

Purpose

The purpose of the policy is to ensure that staff and student data is collected and used fairly and lawfully. The Institute is committed to ensuring that every member of staff and registered student complies with the Data Protection Act 1998 regarding the confidentiality of any personal data held by the Institute in whatever form.

Global Alliance Academy is committed to ensuring the privacy and security of personal data in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR). This Data Protection Policy outlines our commitment to protecting the rights and privacy of individuals whose personal data we process.

2. Scope

This policy applies to all employees, the students studying at the institute, contractors, and third parties who process personal data on behalf of Global Alliance Academy.

3. Data Protection Principles

Global Alliance Academy adheres to the following data protection principles:

Lawfulness, Fairness, and Transparency:

We process personal data lawfully, fairly, and transparently, providing individuals with clear information about how their data will be used.

Purpose Limitation:

Personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

Data Minimization:

We only collect and process the personal data that is necessary for the intended purpose.

Accuracy:

We take reasonable steps to ensure that personal data is accurate and kept up to date.

Storage Limitation:

Personal data is stored for no longer than necessary for the purposes for which it is processed.

Integrity and Confidentiality:

We implement appropriate security measures to protect personal data from unauthorized access, disclosure, alteration, and destruction.

Accountability:

We are accountable for our data protection practices and can demonstrate compliance with data protection laws.

4. Data Subject Rights

Individuals whose personal data is processed by Global Alliance Academy have the following rights:

Right to be Informed

Right of Access

Right to Rectification

Right to Erasure

Right to Restrict Processing

Right to Data Portability

Right to Object

Rights in Relation to Automated Decision Making and Profiling

Requests related to these rights should be directed to the Data Protection Officer.

5. Data Security Measures

Global Alliance Academy implements appropriate technical and organizational measures to ensure the security of personal data. This includes measures to prevent unauthorized access, disclosure, alteration, and destruction of personal data.

6. Data Breach Response

In the event of a data breach, Global Alliance Academy will promptly assess the breach, take necessary steps to mitigate its impact, and notify the relevant supervisory authority and affected individuals as required by law.

7. Data Protection Officer

Global Alliance Academy has appointed a Data Protection Officer (DPO) who is responsible for ensuring compliance with this policy and applicable data protection laws. The DPO can be contacted at [insert contact details].

8. Training and Awareness

Employees and relevant third parties are provided with training and awareness programs to ensure understanding and compliance with this Data Protection Policy.

Student and employee data

The data collected from students and employees is treated with confidentiality and is shared only with staff directly involved with the processing of the application as per the provisions of the Data Protection Act and FOI legislation. Any other data collected during their lifecycle at the institute is processed confidentially and lawfully. Information about a data subject may be disclosed to other bodies as required by law, for crime prevention or detection purposes, or to comply with our obligations as a sponsor of migrants licensed by the UK Border Agency. Disclosures will also be made by the Institute as outlined below:

(a) to other higher education institutions or awarding bodies, where students are involved in validated programmes or courses;

(b) authorised bodies such as sponsors and agencies (eg the Home Office, Quality Assurance Agency), information sharing partners and present/ potential employers;

(c) names included in pass lists, displayed on noticeboards and/ or in the publication of awards;

(d) use or publication of personal email addresses on the institute's website. This means that the information will be available worldwide, including in countries where the rights of data subjects are not protected by law. If you wish, you may opt to have your address withheld by emailing **info@globalallianceacademy.co.uk**.

In the event the Institute needs to share the data subject's data with a third party the data subject's permission is sought beforehand.

The data is stored in electronic form as well and the same level of privacy and confidentiality is applied as provided in Data Protection Act 1998 and FOI legislation.

Collection of student data using Biometric Device

As part of an upgrade of its systems, the Institute has decided to collect biometric data in the form of a fingerprint.

This data will be used for attendance monitoring, related administration and statistics, and other legitimate reasons. It will be held securely and in accordance with the Data Protection Act 1998. Biometric data will not be shared with any third parties except as necessary to operate the technology or as ordered by law. Information derived from it (for example statistics) will be passed to the UK Border Agency where required; and may be shared with higher education, supervising or awarding bodies and other organisations where there is an obligation or it is lawful to do so.

Use of CCTV

The Institute has installed a CCTV network to ensure the safety and security of its employees and students. The CCTV equipment however does not use any automated software i.e., for face recognition or gait recognition. The CCTV has a

clear and limited purpose of monitoring the activities of the staff and students of the Institute. The images captured are not shared with any third party except in the cases of crime detection or helping police for any investigation. The CCTVs are fixed at visible places from where only images fit for the purpose can be captured.

Responsibilities of employees in charge of student and employee data

Employees who are in charge of collecting, holding, and processing personal data are apprised of the legal requirements of data protection. The Human Resources department of the Institute organises induction for new recruits and disseminates guidelines for the proper use of personal data to all employees from time to time. The Institute ensures that employees are:

- aware that all personal data collected, held, and processed, including via Internet and software are subject to the Data Protection Principles,
- aware of the circumstances under which they may legitimately access, process and disclose personal data of the students in the course of their employment
- accessing the data only for a purpose which is explicit, valid and necessary
- aware that any breach of the Data Protection policy may result in disciplinary procedures being instigated against them

Collection and processing of personal data relating to a disability or health condition

The Institute positively encourages the disclosure of disabilities or health conditions to ensure that reasonable adjustments are made to meet the needs of individual students and employees. Non-disclosure of disability may result, in some cases, in the Institute being unable to appropriately meet individual needs. The Institute believes all data subjects have the right to confidentiality to protect their interests and ensure a relationship of trust between student and staff and among colleagues. It is the policy of the Institute that no information regarding a student's or employee's disability shall be shared either directly or indirectly with any other department of the Institute, or any external agency or person, without that data subject's prior, expressed consent; except where issues of safety or legality apply.

Data of students with criminal convictions

Information relating to the criminal convictions of a data subject is treated confidentially and only released to relevant staff whenever necessary. Where it is decided that staff other than those responsible for the data need to be given information about a data subject's criminal conviction, the data subject will be informed that information is being passed on and to whom. Convictions that are spent (as defined by the Rehabilitation of Offenders Act 1974) are not considered to be relevant and a data subject is not required to reveal them.

Use of personal data in research

The Data Protection Act 1998 exempts personal data used for research purposes from certain protection rules. If the purpose of the research processing is not measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject, the data can be processed for purposes other than for which it was originally obtained. The personal data collected for research purposes can be held indefinitely. Data collected fairly and lawfully for the purpose of one piece of research can be used for other research, providing that the final results of the research do not identify the individual. Such data must not be processed to support measures or decisions with direct consequences for the individuals concerned, or in a way, which is likely to cause substantial damage or distress to any data subject.

Seeking consent of students

A data subject is required to sign a declaration at the time when the application is made giving consent to the storage and processing of the data provided with the application to be used by the institute under the provision of the Data Protection Act 1998.

The applicant must tick the box in the criminal conviction section on the monitoring form if either of the following statements applies to him/her:

- has a relevant criminal conviction that is not spent
- is serving a prison sentence for a relevant criminal conviction.

At any time the data subjects are required to sign a declaration giving consent to the storage and processing of the data for a particular purpose if the consent for that purpose is not sought previously.

Back-up of personal data

The Institute has put in place provisions for frequent back-up or duplicate copies of all personal data produced in personal data processing operations. The data is securely stored from the primary data source within the Institute and off-site.

There are designated personnel tasked with the responsibility of ensuring the recovery of personal data, and establishing its accuracy and integrity, within a reasonable time following any disaster which might result in the loss of data from the primary source.

Alumni records

Normally student records will be destroyed after a certain period as is detailed in the Records retention policy of the Institute, however, personal details of alumni will be stored in the alumni database for a longer period. While collecting Alumni data the Institute ensures that students are informed about the purpose of that collection of the data, i.e. that the Institute will wish to maintain contact with them after they finish their course of study. The students can opt-out at any time by forwarding the opt-out request to **info@globalallianceacademy.co.uk**.

Disclosure of data to third parties

The Institute ensures that personal data under its control is not disclosed to unauthorised third parties.

Unauthorised third parties will include:

- A person or organisation to whom the data subject has not consented that the data be disclosed unless the 1998 Act expressly permits such transfers without such consent
- A person or organisation to whom the data subject has consented that the data be disclosed, but where the request is for reasons other than that for which the data was collected, or for which the consent was given, unless the 1998 Act expressly permits such transfers without such consent

- "Unauthorised third parties" will include family members, friends, local authorities, government bodies, and the police, unless disclosure is exempted by the 1998 Act, or by other legislation. There is no general legal requirement to disclose information to the police.

Data may be disclosed to third parties without consent, in amongst other circumstances, situations where it is required for the:

- purpose of protecting the vital interests of the data subject (i.e. release of medical data where failure to release the data would result in harm to, or the death of, the data subject)
- purpose of preventing serious harm to a third party that would occur if the data were not disclosed
- purpose of safeguarding national security
- prevention or detection of crime
- apprehension or prosecution of offenders
- assessment or collection of any tax or duty or any imposition of a similar nature
- discharge of regulatory functions, including securing the health, safety and welfare of persons at work

Publication of Information relating to Staff and Students of the Institute

It is the policy of the Institute to make public as much information about the Institute as possible. The information can be published in printed, electronic or any other form. This includes but is not limited to:

- Organisational structure showing roles and names
- List of members of staff
- Photographs of members of staff
- List of students to whom awards have been made or are likely to be made by the Institute

Any individual who wants his details not to be included in the above-referred lists or categories to remain confidential should contact the Associate Dean.

Data Protection Act Registration

The Data Protection Act requires the Institute to notify the Data Protection Commissioner of the personal data the Institute holds about individuals. The Institute is registered under the registration No. ZA644294.

Policy Review and Updates

This Data Protection Policy is subject to periodic review to ensure ongoing compliance with data protection laws and regulations. Updates will be communicated to all relevant parties.

Contact Information

For any questions or concerns related to data protection, please contact the Data Protection Officer at info@globalallianceacademy.co.uk

Review

The policy is reviewed every year

.

Approval and Adoption

This Data Protection Policy has been approved and adopted by the Global Alliance Academy.

Date of Approval 21 09 2023