Data Protection Policy

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 ensure 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.

Scope

The policy applies to all members of staff, the students studying at THE INSITIUTE and any visiting member of the public who comes in contact with any kind of personal data.

General Policy

The Institute stores necessary data about its past, current and potential employees and students, visiting faculties and other users of the institute facilities to run its day-to-day operations smoothly and effectively. The data collected from students and employees is treated with confidentiality and is shared only with staff directly involved with the processing of the stored data as per the provisions of the Data Protection Act and Freedom of Information (FOI) legislation. Any other data collected during the lifecycle of students or employees

at the institute is processed confidentially and lawfully. Data collected and held should be adequate, relevant and not excessive in relation to the purposes for which it has been collected. All data must be deleted or destroyed when no longer required. Staff data is stored in order to process information so that THE INSITIUTE can recruit and pay staff, organise programmes and to comply with QAA and other external bodies and government departments.

Data Protection Act 1998 Principles

The Institute adheres to the principles of the Data Protection Act which are followed and fully applied to personal data:

1. Data is processed fairly and lawfully
2. Data is obtained and processed for specific purposes
3. Data is adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
4. Data is accurate and kept up to date
5. Data is not kept for longer than is necessary
6. Data is processed in accordance with the rights of the data subject
7. Data is kept securely
8. Data is not transferred outside the EU or the European Economic Area unless the country in question has an adequate level of protection for data subjects.

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 in order 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 initiate'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 the purposes of 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 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 Institute has designated security staff and IT professionals who monitor the CCTV equipment. The operators of the equipment are made aware of the legal requirements of the use of images. 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 the 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 condition 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 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.

Data Security standard

The Institute meets ISO/IEC 27001 standard. ISO/IEC 27001 is an Information Security Management System (ISMS) standard which provides a high level of compliance with the 1998 Act and ensures that the level of data security in place in the Institute is appropriate to the risks represented by the processing and the nature of the data to be protected. The Institute systematically examines its information security risks, taking account of the threats, vulnerabilities and impacts and has the acceptable means in place to address those risks. This involves adopting the right design and implementation of information security controls with regular ongoing management to ensure that these security needs are always met.

The following measures are taken to protect data from unauthorised access or viewing:

1. Computer screens which are used by staff to access personal data are not placed in public areas where unauthorised persons can view the screen content
2. CDs, flash drives or any other electronic media and hard copies are kept at secure places away from public areas.
3. Unwanted printed material is shredded and disposed of ensuring no misuse of data. Unwanted data in electronic form is permanently erased.

4. Biometric data is stored in an encrypted format which cannot be viewed in a human understandable form. Biometric data is used only to register student attendance in order to ensure that no student misrepresents or identifies himself as a different student.
5. All computer systems which are used to process personal data are password controlled. Computer screens are kept locked when the user of the machine is away or is turned off when not in use.

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.

Examination scripts

Examination scripts are expressly exempted from the data subject access rules. The Institution is under no obligation to permit examination candidates to have access to either original scripts or copies of the scripts. However, a student has the right to request a copy or summary "in intelligible form" of the Internal or external examiners' comments, whether made on the script or in another form that allows them to be held and applied to the original script (e.g. in a coded

table). The request is provided within the stipulated timescale of 40 days. However, in the case of examinations if a request is made before results are announced, there is a limit of five months from the request or 40 days from the announcement of the result, whichever is earlier.

Examination board minutes and related documentation

Minutes of Examination Boards that contain discussion about a student will be subject to data subject access where the student is named, or referred to by identifiers from which the student may be identified (such as the institute student ID or validating university's ID), unless the data cannot be disclosed without additionally disclosing personal data about a third party. However, if the third party gives consent to the disclosure or the information can be provided by easily withholding third party data, the requested information will be provided to the student.

Alumni records

Normally student records will be destroyed after certain period as is detailed in Records retention policy of the Institute, however, personal details of alumni will be stored in the alumni database for 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 are able to 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 of 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
- Members of the Council, Academic Board and other committees
- 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. Z8669010.

Review

The policy is reviewed on a yearly basis

.