

GENERAL DATA PROTECTION REGULATION POLICY



1. General Statement of the Centre's Duties

The Centre is required to process relevant personal data regarding employees or students as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

The Centre will comply with:

The terms of the 2018 General Data Protection Regulation, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful

2. Data Protection Controller and Processor

The Centre has appointed the Head of Centre (Kate Towers) as the Data Protection Controller and Processor (Charlotte Towers) who will endeavour to ensure that all personal data is processed in compliance with this Policy, the Principles of the General Data Protection Regulation 2018.

3. The principles

The Centre shall so far as be reasonably practicable comply with the Data Protection Principles ("the Principles") contained in the General Data Protection Regulation to ensure all data is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

GENERAL DATA PROTECTION REGULATION

POLICY

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Personal Data

Personal data covers both facts and opinions about an individual. It includes information necessary for tuition and employment such as the student's/employee's name and address and details for invoicing and payment of wages.

How we handle personal data is set out in our Fair Processing Policy which is available on our website or from reception.

Data Storage

Personal data will be stored in a secure and safe manner.

- Electronic data will be protected by standard password and firewall systems operated by the Centre.
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception.
- Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- Particular attention will be paid to the need for security of sensitive personal data.

5. Processing of Personal Data

Documentation provided by agencies for the referral of a student to Tower Learning Centre falls under the definition of personal data and is not otherwise exempt will remain confidential and will only be disclosed to third parties with the consent of the employee. The Centre aims to process and secure data within 48 hours after receiving it. An employee's consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which

GENERAL DATA PROTECTION REGULATION

POLICY

falls under the definition of personal data and is not otherwise exempt will remain confidential and will only be disclosed to third parties with the consent of the employee.

6. Sensitive Personal Data

The Centre may, from time to time, be required to process sensitive personal data regarding an employee/student. Sensitive personal data includes medical information and data relating to religion, race, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by the Centre, the explicit consent of the employee will generally be required in writing.

7. Rights of Access to Information

All employees/students and agencies have a right of access to information held by the Centre, subject to the provisions of the General Data Protection Regulation 2018. Any employee wishing to access their personal data should put their request in writing to the Head of Centre. The Centre will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 30 days for access to records and 21 days to provide a reply to an access to information request. The information will be imparted to the employee as soon as is reasonably possible after it has come to the Centre's attention.

Subject Access Requests If the Centre receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the Centre will respond within the 30-day deadline.

Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 30-day time limit.

8. The right to erasure

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;

GENERAL DATA PROTECTION REGULATION

POLICY

- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

When does the right to erasure not apply?

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

9. Right to Restrict Processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, we are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- You have one calendar month to respond to a request.
- This right has close links to the right to rectification and the right to object

GENERAL DATA PROTECTION REGULATION

POLICY

10. The Right to Data Portability

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

11. Exemptions

Certain data is exempted from the provisions of the General Data Protection Regulation which includes the following:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Centre.

The above are examples only of some of the exemptions under the regulation. Any further information on exemptions should be sought from the Data Protection Controller

GENERAL DATA PROTECTION REGULATION

POLICY

12. Accuracy

The Centre will endeavour to ensure that all personal data held in relation to employees/students is accurate. Employees must notify the Data Protection Controller of any changes to information held about them. An employee has the right to request that inaccurate information about them is erased.

13. Enforcement

If an employee/student or agency believes that the Centre has not complied with this Policy or acted otherwise than in accordance with the General Data Protection Regulation, they should utilise the company grievance procedure and should also notify the Data Protection Controller