FIRST CLASS

TAILORED SOLUTIONS FOR YOUNG PEOPLE

Data Protection Policy

Reviewed: Apr 2020
Next review date: Apr 2021

Data Protection Policy

The Data Protection Act (DPA) 2018 is the law that protects personal privacy and upholds individual's rights and is the UK's implementation of the General Data Protection Regulation (GDPR). It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information kept by First Class Tailored Solutions (FCTS) is dealt with properly and securely and in accordance with the DPA 2018. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1. Scope of the Policy

Definitions:

- Data Subject, an individual who is the subject of personal data
- Data Controller is FCTS and they determine the purpose and means by which personal data is processed.
- Data Processor is anyone who processes personal data on behalf of the Data Controller
- Data Protection Officer (DPO) duties include advising on data protection obligations, monitoring internal compliance and providing advice on data protection impact assessments.

a. Personal Data:

Covers both facts and opinions about an individual where that data identifies an individual. For example, it includes data necessary for employment such as the staff member's name, address and details for payment of salary or a learner's attendance record, record on ongoing sessions and exam results. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings. Personal data may also include sensitive personal data as defined in the above Act.

b. Sharing Data

FCTS collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the company. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

c. Processing of Personal Data:

Consent may be required for the processing of personal data unless it is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

Learner consent to process their data and disclose it to parents is implicit when they reach the age of 18. If a pupil wishes to revoke or change consent they must agree a specific agreement on how their data is to be processed by a Data Processor.

d. Sensitive Personal Data:

FCTS will, from time to time, be required to process sensitive personal (special category) data, which includes data relating to medical information, gender, religion, race, sexual orientation, health and ethnic background. This data can also covers politics, genetics, biometrics, sex life and trade union membership. This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

e. Rights of Access to Information:

Data subjects have the right of access to information held by FCTS, subject to the provisions of DPA and the Freedom of Information Act 2000. Any data subject wishing to access their personal data should put their request in writing to the Data protection Officer at FCTS. A search will be conducted of the data storage in our management information systems. Any compliance with the request should be completed within 1 month. Any delay to this timescale should be communicated to the individual requesting it, prior to the 1-month deadline.

f. Data *Retention/Deletion*:

FCTS will archive personal data for a law enforcement purpose where the processing is necessary for statistical/educational purposes. All email data can be assigned a retention date, applicable to individual or folder email content. All FCTS personal data is stored on Office 365 within OneDrive, Teams or SELIMS and is archived or deleted. Personal data shall be archived or disposed of appropriately and in accordance with best practise.

2. The Data Protection Principles for personal data processing

The GDPR sets out the principles that must be adhered to for all processing of personal data. Personal data shall be:

a. processed lawfully, fairly and in a transparent manner.

   All processing of personal data shall be in accordance with UK and EU law, and only take place to the extent that one of the following applies:

i. the data subject has given their consent.
ii. the processing is necessary for the performance of a contract.
iii. the processing is necessary for compliance with a legal obligation.
iv. the processing is necessary to protect the vital interests of the data subject.
v. the processing is necessary either for a task carried out in the public interest or in the exercise of the data controller's official authority.

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

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d. accurate and, where necessary, kept up to date.

e. kept in a form that permits identification for no longer than is necessary for the purposes for which the data are processed.

f. processed in a manner that ensures appropriate security of the personal data.

3. Responsibilities

3.1 FCTS must:

- Manage and process personal data properly for students and employees, both past and present. Job applicant information is also included.
- Protect the individuals' right to privacy
- Provide an individual with access to all personal data held on them.

3.2 FCTS has a legal responsibility to comply with the Act and Regulation. The company, as a corporate body, is named as the Data Controller under the Act and Regulation.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act and Regulation.

3.3 FCTS is required to 'notify' the Information Commissioner of the processing of personal data and is registered with the ICO (ZA310273)

3.4 Every Data Processor should ensure that all sensitive personal data is kept under a secure means and is to comply with the DPA when managing that information.

3.5 When introducing a new processing activity that is likely to result in a high risk to the rights and freedoms of individuals FCTS will undertake an impact assessment to

identify and mitigate those risks, and seek guidance from the Data Protection Officer if required.

3.6 All breaches that present a risk to the rights and freedoms of individuals, as determined by the data Protection Officer, shall be reported to the Information Commissioner at the earliest opportunity and in any event no later than 72 hours from discovery. FCTS will try to ensure that all data is kept secure and identify where this has not been the case. Where a breach represents a high risk to individuals FCTS shall notify all data subjects concerned.

3.7 Security of all FCTS data is vital and is stored on secure servers located in the UK, which are GDPR compliant.