Bristol Tuition Centre

GDPR and Data Protection Policy

Version 4

Policy name	Owned by	Ratified by	Date	Review date
GDPR and Data Protection Policy	Swindon Tuition Centre	Jo Vertannes	6.09.2018	6.09.2019

Policy Updates

Review date	Update Summary	Reviewed by:	Next Review:
6.09.2019	N/A	J.Vertannes	6.09.2020
30.07.2020	Legislative updates across policy.	J.Vertannes	4.09.2021
4.09.2021	Updated privacy notices and website banners.	J.Vertannes	4.09.2022
Sept 2023	Reviewed		Sept 2024

Introduction

Data Protection is about safeguarding how people's personal information is used by organisations, businesses and the government. The General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data. In the UK we continue to follow the Data Protection Act 2018 even though we have left the European Union (EU).

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

- The Centre as the Data Controller will comply with its obligations under the GDPR and DPA. The Centre is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

- All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

- Bristol Tuition Centre is classed as a data controller however individuals who are subcontracted are also classed as data controllers. Swindon Tuition Centre will only appoint data processors who can provide guarantees that the requirements of the law and the procedures outlined in this policy will be met and in turn the right of data subjects will be protected.

Scope of the Policy

All employees, tutors and students; Internal Quality Assurance of any GDPR and Data Protection processes from external agencies and partners.

The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)

4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).

5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)

6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation

1. In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards[2].

2. This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

3. These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

1. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Centre
2. Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering

into a contract
3. Processing is necessary for compliance with a legal obligation to which the data controller is subject
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person
5. Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party

The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent from be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the Centre's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the Centre's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so
- One of the special conditions for processing sensitive personal information applies:

a. the individual ('data subject') has given explicit consent

(which has been clearly explained in a Privacy Notice)

b. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Centre or the data subject

c. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent

d. the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim

e. the processing relates to personal data which are manifestly made public by the data subject

f. the processing is necessary for the establishment, exercise or defence of legal claims

g. the processing is necessary for reasons of substantial public interest

h. the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services

i. the processing is necessary for reasons of public interest in the area of public health.

The Centre's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the Centre can rely on another legal basis of processing, explicit consent is usually

required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the Centre can demonstrate compliance with the GDPR.

Data Protection Impact Assessment (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the Centre's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- a) whether the processing is necessary and proportionate in relation to its purpose
- b) the risks to individuals
- c) what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Centres from the DfE with reference to the DPIA template. When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

Documentation and records

Written records of processing activities must be kept and recorded including:

- a) the name(s) and details of individuals or roles that carry out the processing
- b) the purposes of the processing
- c) a description of the categories of individuals and categories of personal data •
- d) categories of recipients of personal data

- e) details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

- f) retention schedules
- a description of technical and organisational security measures.

As part of the Centre's record of processing activities the DPO will document, or link to documentation on:

- a) information required for privacy notices
- b) records of consent
- c) controller-processor contracts
- d) the location of personal information;
- e) DPIAs and
- f) Records of data breaches.

Records of processing of sensitive information are kept on:

- a) The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- b) The lawful basis for our processing and
- c) Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The Centre should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- 1. Carrying out information audits to find out what personal information is held •

2.. Talking to staff about their processing activities

- 3. Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notice

The Centre will issue privacy notices as required, informing data subjects (or parents/carers of children and young people) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the Centre will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The Centre must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The Centre will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The Centre will issue a minimum of two privacy notices:

1. Privacy Notice for Pupils, Customers and Providers
2. Privacy Notice for Employees, Workers and Contractors

Both Privacy Notices include details of how to complain if you have any concerns about use of your personal information internally and externally.

These will be reviewed in line with any statutory or contractual changes.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The Centre maintains a Record Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all

personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Appendix 1 - Procedure for Access to Personal Information)*

- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the Centre no longer need the personal information, but you require the data to establish, exercise or defend a legal claim

- To restrict the processing of personal information temporarily where you do not think it is accurate (and the Centre are verifying whether it is accurate), or where you have objected to the processing (and the Centre are considering whether the Centre's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

- To withdraw consent to processing at any time (if applicable)

- To request a copy of an agreement under which personal data is transferred outside of the EEA.

- To object to decisions based solely on automated processing, including profiling

- To be notified of a data breach which is likely to result in high risk to their rights and obligations

- To make a complaint to the ICO or a Court.

Individual Responsibilities

During employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The Centre expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes

- only allow other staff to access personal information if they have appropriate authorisation

- only allow individuals who are not Centre staff to access personal information if you have specific authority to do so

- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the Centre's policies).

- not remove personal information, or devices containing personal information (or which can be used to access it) from the Centre's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device

- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security

The Centre will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their Centre's acceptable usage policy.

The Centre will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Centre has implemented and maintains in accordance with the GDPR and DPA.

Where the Centre uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

1. the organisation may only act on the written instructions of the Centre
2. those processing data are subject to the duty of confidence
3. appropriate measures are taken to ensure the security of processing

4. sub-contractors are only engaged with the prior consent of the Centre and under a written contract/ Service Level Agreement

5. the organisation will assist the Centre in providing subject access and allowing individuals to exercise their rights in relation to data protection

6. the organisation will delete or return all personal information to the Centre as requested at the end of the contract

7. the organisation will submit to audits and inspections, provide the Centre with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Centre immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information

Personal data will be kept securely in accordance with the Centre's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Personal information that is no longer required will be deleted in accordance with the Centres Record Retention Schedule.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored

- Unauthorised access to or use of personal information either by a member of staff or third party

- Loss of data resulting from an equipment or systems (including hardware or

software) failure

- Human error, such as accidental deletion or alteration of data

- Unforeseen circumstances, such as a fire or flood

- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams

- Blagging offences where information is obtained by deceiving the organisation which holds it

The Centre must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The Centre must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Executive Head Teacher/Head of Centres immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the Centre's agreed breach reporting process.

Training

The Centre will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

The Centre takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the Centre and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the Centre's procedures and this action may result in dismissal for gross misconduct. If a non employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the Centre's DPO: Rachel Barnes rachel@swindontuitioncentre.co.uk.

Review of Policy

This policy will be updated as necessary to reflect best practice amendments made to the GDPR or DPA. At a minimum it will be reviewed annually.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The Centre is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway. **Explicit Consent:**

consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, and an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Centre collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, Centre workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.