Brightpath Education Services Limited
GDPR and Data Protection Policy

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.

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

Brightpath Education Services as the Data Controller will comply with its obligations under the GDPR and DPA. The Company 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.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the Company and all staff comply with the legislation.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The Company collects personal data including names and contact details of individuals.

The Principles

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

[1] GDPR Article 4 Definitions

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**).

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:

- 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 Company

- 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

- Processing is necessary for compliance with a legal obligation to which the data controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[2]

[2] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

- 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 Company's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the Company'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[3] 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.

Brightpath Education Services Limited does not collect sensitive personal information.

Data Protection Impact Assessments (DPIA)
All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the Company'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.

[3] GDPR, Article 9

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:

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

Documentation and records

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

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- retention schedules
- a description of technical and organisational security measures.

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

- Carrying out information audits to find out what personal information is held

Privacy Notice

The Company will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) 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.

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 Company maintains a 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. The Company will take all reasonable steps to destroy or delete all personal data that is held when it is no longer required in accordance with the Schedule.

The Company will 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
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;

- 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;

- 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 Company 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 Company is verifying whether it is accurate), or where you have objected to the processing (and the Company is considering whether the Company'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 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.

Information Security
The Company 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.

The Company 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.

The Company 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.

Storage and retention of personal information
Personal data will be kept securely in accordance with the Company'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 Company's 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 Company 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 Company must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

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.