Data Protection Policy

Purpose

The policy and associated procedures aim to ensure Blueprint Education Services Ltd explain the responsibilities of staff under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). Blueprint Education Services Ltd is committed to being transparent, lawful, and fair about how it collects and uses the personal data of its workforce, customers, and stakeholders to ensure it meets data protection obligations. This policy sets out our commitment to data protection together with rights and obligations in relation to personal data.

Scope

This policy applies to the collection, processing, and disposal of all personal and special category data in connection with the work, studies, or other activities in association with Blueprint Education Services Ltd and any of its subsidiary companies. This includes data that enters the public domain through social networking sites and emails; the security of data transferred via these methods is also subject to the same data protection requirements. The policy sets out the expected behaviours of all Blueprint Education Services Ltd Directors, employees, associates or anyone working on Blueprint Education Services Ltd premises or on our behalf.

Policy Statements

1. Data Protection Law

This policy is informed by and meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018

(DPA 18) and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator.

2. The Data Controller

Blueprint Educations Services Ltd is the data controller, and the company is ultimately responsible for the implementation of all appropriate policies and procedures to meet its obligations. Employees, associates or anyone working for Blueprint Education Services Ltd are required to implement the policy on behalf of the business and are referred to throughout this document as 'staff'.

3. The Data Protection Officer

'Blueprint Education Services' Data Protection Officer is Director Olivier Playe. Their contact details are published on our website, as well as being widely available to all employees of Blueprint Education Services Ltd.

4. Data Protection Business Partners

Blueprint Education Services has Data Protection Business Partners, each of whom supports the Data Protection Officer on a particular aspect of data protection:

- CEO Jason Folkett
- Director of Finance Nathan Gillott
- Director of Commerce Colin Marshall

5. Data Protection Principles

Blueprint Education Services Ltd complies with the six data protection principles that guide data protection legislation. In summary, we require that personal data is:

1. Processed fairly, lawfully, and in a transparent manner.
2. Used only for limited, specified, stated purposes, and not used or disclosed in any way incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary.

4. Accurate and, where necessary, up to date.
5. Not kept for longer than necessary.
6. Kept safe and secure. In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data.

Failure to do so can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to policies, operational procedures, and guidance to give them appropriate direction on the application of data protection legislation.

6. Lawful Use of Personal Data

To collect and/or use personal data lawfully, BES must show the processing is lawful, fair, and transparent. It is not enough to show the processing is lawful if it is fundamentally unfair or hidden from the individual concerned. In addition, when the BES collects and/or uses special categories of personal data, the business must show that one of a number of additional conditions is met. BES will carefully assess how it uses all personal data and document this within the Information Asset Register. If BES changes how it uses personal data, BES must update this record and may also need to notify individuals about the change. Any changes to the use of personal data must therefore be approved by the Data Protection Officer in advance and documented through an update to the Asset Register and Retention Policy, if applicable. When collecting data BES will capture and retain consent, together with the version of the privacy information that accompanied the consent. If the legal basis for processing data is based on consent BES must respect the individual's right to withdraw consent at any time.

7. Transparent Processing – Privacy Policy

Where BES collects personal data directly from individuals, BES will inform them about how their personal data is used through the appropriate Privacy Policy published on the BES website. If BES changes how it uses personal data, BES may need to notify individuals about the change. If staff, therefore, intend to change how they use personal data they must notify the Data Protection Officer, who will decide whether the intended use requires amendments to be made to the Privacy Policy and any other controls which need to apply.

8. Data Quality

Data Protection Laws require that BES only collects and processes personal data to the extent that it is required for the specific purpose(s) notified to the individual in a Privacy Policy and as set out in the BES Information Asset Register. BES is also required to ensure that the personal data held is accurate and kept up to date. All staff that collect and record personal data shall ensure that the personal data is recorded accurately, is kept up to date, and shall also ensure that they limit the collection and recording of personal data to that which is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. All staff that obtain personal data from sources outside BES shall take reasonable steps to ensure that the personal data is recorded accurately, is up to date, and is limited to that which is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require staff to independently check the personal data obtained.

BES quality measures include:

• Correcting personal data in a timely manner that is discovered to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the individual does not request rectifications.

• Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.

• The removal of personal data if in violation of any data protection principles, or if the personal data is no longer required.

BES recognises the importance of ensuring that personal data is amended, rectified, erased, or its use restricted where this is appropriate under Data Protection Laws.

9. Data Security

BES takes information security very seriously and has policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure data is not accessed except by employees in the proper performance of their duties. Please see the Information Security Policy and IT Acceptable Use Policy for further details.

10. Contracts and Third-Party Arrangements to Access the College's Personal Data

If the BES appoints a third party involving the processing of the BES personal data, the BES can only appoint them where sufficient due diligence has taken place and only where the BES has an appropriate contract in place. The contract must have a duty of confidentiality and must implement appropriate technical and organisational measures to ensure the security of data. The contract must be in writing and approval for signatory must be granted from the CEO.

BES is considered as having appointed a Data Processor when we engage someone to perform a service for us and, as part of that service, they may get access to the College's personal data. BES, as the Data Controller, remain responsible for what happens to the personal data.

Data Protection Law requires all contracts with a Data Processor to contain the following obligations as a minimum:

• To only act on the written instructions of the Data Controller.

• To not export personal data without the Controller's instruction.

• To ensure staff are subject to confidentiality obligations.

• To take appropriate security measures; to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract.

• To keep the personal data secure and assist the Controller to do so; to assist with the notification of data breaches and Data Protection Impact Assessments.

• To assist with subject access/individual rights.

• To delete/return all personal data as requested at the end of the contract; to submit to audits and provide information about the processing.

• To tell the Controller if any instruction is in breach of Data Protection Law.

In addition, contracts between Chesterfield College and any Data Processor should set out:

• The subject matter and duration of the processing.

• The nature and purpose of the processing.

• The type of personal data and categories of individuals.

• The obligations and rights of the Controller

11. Data Protection by Design

To meet the requirements of Data Protection Law and protect the rights of data subjects, BES is responsible for implementing appropriate technical and organisational measures, such as pseudonymisation and data minimisation, in an effective way to ensure the necessary safeguards for processing before we can commence processing and at the time of the processing itself.

When designing new systems or processes, and/or reviewing or expanding existing systems or processes, each will go through an approval process

before continuing. A Data Protection Impact Assessment will be conducted which will allow the BES to assess the impact of the new or altered processing operations on the protection of personal data.

12. Data Protection Impact Assessment (DPIA)

Staff must ensure a Data Protection Impact Assessment (DPIA) is completed where a type of processing, in particular processing using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of an individual. It is important to conduct a DPIA to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations to ensure compliance with approved codes of conduct, special category or criminal conviction data, views of the data subject before the intended processing, and in the interests of the security of the processing operation. This process, supported by the Data Protection Team, will include the purposes for which the activity is carried out, the risks to individuals, and the measures that can be put in place to mitigate the risks.

13. Subject Access Requests and Administration of Individual Rights

Individuals have the right under Data Protection Law to ask BES to confirm what personal data is held about them by making a Subject Access Request. All Subject Access Requests will be directed to the Data Protection Team who will ensure that the agreed procedure is followed to establish the identity of the individual, the scope of their request, and the timely provision of a response.

BES will not charge a fee for the processing of a Subject Access Request but reserves the right to pass on the cost of providing additional or repeat copies of the same information, as well as the cost of meeting any manifestly unfounded or excessive requests.

Situations may arise whereby providing information requested may disclose personal data about another individual. In such cases, information will be redacted or withheld as necessary to protect that person's rights.

Individuals have a number of rights which they can exercise with regards to the processing of their personal information. BES will investigate and respond without undue delay, and at least within one month of the notification, where appropriate, with supporting action taken.

14. Right of Erasure (Right to be Forgotten)

This is a limited right for individuals to request the erasure of personal data concerning them where:

• The use of the personal data is no longer necessary.

• Their consent is withdrawn and there is no other legal ground for the processing.

• The individual objects to the processing and there are no overriding legitimate grounds for the processing.

• The personal data has been unlawfully processed.

• The personal data must be erased for compliance with a legal obligation.

BES will respond to all requests for data erasure within 30 days and will confirm what categories of personal data have been erased, as well as any categories of data retained where they do not fall within the scope of this right.

In a marketing context, where personal data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the personal data will be erased or, if also retained for another legitimate reason, clearly annotated to prevent future use for marketing purposes.

15. Right of Data Portability

An individual has the right to request that data concerning them is provided to them in a structured, commonly used, and machine-readable format, where the processing is based on consent or a contract, and the processing is carried out by automated means. This right is not the same as Subject Access and is intended to give individuals a subset of their data. BES will respond to all requests to provide portable data within 30 days, providing either a suitable dataset for transport or a detailed explanation as to why the request cannot be fulfilled.

16. Right of Rectification and Restriction

Individuals are also given the right to request that any personal data is rectified if inaccurate and to have use of their personal data restricted to a particular purpose in certain circumstances. BES will use all personal data in accordance with the rights given to individuals under Data Protection Laws and will ensure that it allows individuals to exercise their rights in accordance. The Data Protection Officer will investigate any cases where an individual feels that their rights, including to the rectification of incorrect information or the restriction of use, have not been met.

17. Marketing and Consent

BES will sometimes contact individuals to send them marketing or to promote BES. Where BES carries out any marketing, activities will be carefully planned to ensure compliance with Data Protection Law and other applicable legal and regulatory frameworks. For any advertising or marketing communication directed to individuals using their personal information, BES will operate within a framework of consent and maintain records within its central systems for student records and customer relationship management. For electronic marketing, BES will provide a clear and simple opt-in system for individuals, with a simple means to withdraw consent at any time. Where contact information is collected face-to-face or by telephone, or electronic

communication, and as part of a specific marketing activity, BES will use a 'soft opt-in' record of consent and provide the individual with an opportunity to opt-out on all occasions that the information is used.

18. Automated Decision Making and Profiling

BES does not carry out automated decision making or profiling in relation to its employees or clients.

19. International Data Transfers

BES does not transfer information internationally. Should staff need to use their approved laptops to access data from outside of the UK they must seek approval from the data protection officer and or the client.

20. Records Management

BES has a legal responsibility not to keep personal data for longer than needed for the specific purposes agreed when it was collected. At the end of the agreed period for each type of information, BES will take steps to delete such information from its information systems, databases, and electronic files, and to destroy paper records using agreed, secure processes.

No client personalised or sensitive data will reside in the BES network or will be held on personalised machines.

21. Data Breach

BES takes information security very seriously. However, it is possible that a personal data breach could occur. A personal data breach is defined as any failure to keep personal data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration, or unauthorised disclosure of personal data. All staff are required to understand the internal reporting process for personal data breaches and comply with the strict timeframes set out within the Data Breach Notification Procedure.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the affected individuals must be notified and provided with information about the likely consequence and the measures for mitigation undertaken.

In accordance with procedure, any high-risk data breach will be reported to the Information Commissioners Office (ICO) immediately upon discovery by the Data Protection Officer, in parallel with a report to the Chief Executive Officer.

All breaches will be investigated formally by the Data Protection Officer and reported to the Directors. Where an investigation identifies a case to be answered by one or more members of staff, this will be addressed.

Where a breach occurs involving the Data Protection Officer, the investigation will be undertaken by the Director of Finance, who will report their findings to the Directors as above.

Implementation

BES will ensure that:

1. The Data Protection Officer will be supported to undertake their duties as identified within our policies.

2. Data protection compliance will be reviewed regularly by the BES Directors against a schedule agreed with the Data Protection Officer.

3. BES staff receive a level of training appropriate to their role, with refresher training annually. This will be recorded and monitored.

4. This policy is available on our website and is monitored and updated regularly.

6. The Data Protection Officer will undertake the minimum prescribed tasks as follows:

- Inform and advise the Board of Directors about all data protection matters and ensure that all staff understand their obligations to comply with Data Protection Laws.

- Monitor compliance with Data Protection Laws, including managing internal data protection activities, advising on Data Protection Impact Assessments, supporting training, and conducting internal audits.

- Be a named point of contact for the ICO and for individuals whose data is processed. Individuals with a complaint about the processing of their personal data is covered by our Freedom of Information policy. should comply with the Complaints and Compliments Policy.

Monitoring

BES has appointed Director Olivier Playe as the designated Data Protection Officer with specific responsibilities and accountability for data protection across the Group.

In discharging their duties, the Data Protection Officer will have a direct line of reporting through the Directors.

The implementation of the Data Protection Policy is continuously monitored by the Data Protection Officer and Directors, who have responsibility for Information Security. The Data Protection Policy is reviewed annually by the BES Directors.

Associated Information and Guidance

Relevant legislation includes:

• Data protection: The Data Protection Act - GOV.UK (www.gov.uk)

• Human Rights Act 1998 (legislation.gov.uk)

• The Data Protection (Processing of Sensitive Personal Data) Order 2000 (legislation.gov.uk)

• Regulation of Investigatory Powers Act 2000 (legislation.gov.uk)

- Freedom of Information Act 2000 (legislation.gov.uk)

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (legislation.gov.uk)

Further guidance:

- The Information Commissioners Office Guide to Data Protection: guide-to-data-protection-1-1.pdf (ico.org.uk)