SB Skills Solutions
Data Protection Policy (DPP)

This Policy should be read in conjunction with all Data Management and Information Governance Policies and related Codes of Practice (CoPs) including:
Information and Data Governance Framework (IDGF)
GDPR & Data Processing Policy & Practice (GDPR)
Information Security Policy (ISP)
Codes of Practice D1 > D14

Privacy Notices
Student Privacy Notice
Website Usage Privacy Notice
Employee Privacy Notice

Compliance & IT Manager (CIM) - Steve Maddocks
Tel: 01695 558420
Email: steve@sbskills.co.uk
or
Senior Information and Risk Officer and Senior Data Protection Officer
Neil Beaumont, Director
Email: neil@sbskills.co.uk

Manager responsible for this document Stephen Maddocks Compliance Manager
Approved On 21/04/2021
Review Date 21/04/2022

SB Skills Solutions
Data Protection Policy

1. Introduction

1.1 SB Skills Solutions needs to collect, store and process personal data in order to carry out its functions and activities. The Company is a **Controller** for most of the personal data it processes and is committed to full compliance with the applicable data protection legislation including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (referred to as the "**GDPR**") and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003.

1.2 GDPR - Up until 24 May 2018, the data protection regime in the UK was governed by the EU Data Protection Directive (95/46/EC) which was implemented in the UK in the form of the Data Protection Act 1998. To address some difficulties arising under the Directive, the EU created a new data protection regime—the General Data Protection Regulation (GDPR). The GDPR replaced the Directive from 25 May 2018. The GDPR is also designed to address technological and societal changes that have taken place over the last 20 years by adopting a technology-neutral approach to regulation. The GDPR contains elements from the previous legislation (i.e. the Data Protection Act 1998), for example, the Data Protection Principles of good practice and the data subject's right to have access to his or her personal data and to correct it where inaccurate. However the GDPR imposes additional requirements.

1.3 This policy should be read in conjunction with the Company's **GDPR & Data Processing Policy & Practice**, **Information Security Policy** and related **Codes of Practice**. These provide more detailed guidance on the correct handling of personal data and together with this policy are an integral part of the overall information governance framework of the Company.

1.4 The Company's Senior Information Risk officer and Data Protection Officer (SIRO & DPO) supported by the Compliance & IT Manager (CIM) are responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the CIM or SIRO/DPO.

2. Scope

2.1 All Company staff, students and other authorised third parties (including temporary and agency workers, contractors, interns and volunteers) who have access to any personal data held by or on behalf of the Company, must adhere to this policy and associated Codes of Practice.

2.2 Personal data means any information relating to an identified or identifiable natural person (referred to as a 'data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

2.3 The information covered by the policy includes all written, spoken and electronic personal data held, used or transmitted by or on behalf of the Company, in whatever media. This includes personal data held on computer systems, hand-held devices, phones, paper records, and personal data transmitted orally.
2.4 We will review and update this policy in accordance with our data protection obligations. We may amend, update or supplement it from time to time and will issue an appropriate notification of that at the relevant time.

3. Data Protection Principles
3.1 The Company will comply with the following data protection principles when processing personal data:

3.1.1 we will process personal data lawfully, fairly and in a transparent manner;

3.1.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

3.1.3 we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;

3.1.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;

3.1.5 we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed;

3.1.6 we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

3.2 The Company is also responsible to demonstrate compliance with the above data protection principles.

4. Basis for Processing Personal Data
4.1 In relation to any processing activity that involves personal data we will, before the processing starts for the first time, and then regularly while it continues:
4.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis for that processing, i.e.:
(a) that the data subject has consented to the processing;
(b) that the 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;
(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;
(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority by the Company; or
(f) where the Company is not carrying out tasks as a public authority, that the processing is necessary for the purposes of the legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
4.1.2 except where the processing is based on consent, satisfy us that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose);
4.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
4.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices; and
4.1.5 where sensitive personal data is processed, also identify a lawful special condition for processing that information (see paragraph 5 below), and document it.

5. Sensitive Personal Data
5.1 Sensitive personal data (sometimes referred to as 'special categories of personal data') are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
5.2 The Company may from time to time need to process sensitive personal data. We will only process sensitive personal data if:
5.2.1 we have a lawful basis for doing so as set out in paragraph 4.2.1 above; and
5.2.2 one of the special conditions for processing sensitive personal data applies, e.g.:
(a) the data subject has given explicit consent;
(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or of 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 relates to personal data which are manifestly made public by the data subject;
(e) the processing is necessary for the establishment, exercise or defence of legal claims; or
(f) the processing is necessary for reasons of substantial public interest.
5.3 The Company's data protection **Privacy Notices** set out the types of sensitive personal data that the Company processes, what it is used for and the lawful basis for the processing.

6. Data Privacy Impact Assessments ('DPIAS' – CoP D4)
Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:
6.1 whether the processing is necessary and proportionate in relation to its purpose;
6.2 the risks to individuals; and
6.3 what measures can be put in place to address those risks and protect personal data.

7. Documentation and Records
7.1 We will keep written records of processing activities. This will be done primarily in the Company's Information Asset Register. Each information asset (which will include personal data) will have an identified Information Asset Owner who will be responsible for the information and for logging a description of the processing on the register. Further details of the Information Asset Register are set out in CoP D3.
7.2 We will conduct regular reviews of the personal data we process and update our documentation accordingly. This may include:
7.2.1 carrying out information audits to find out what personal data the Company holds;
7.2.2 distributing questionnaires and talking to staff across the Company to get a more complete picture of our processing activities; and
7.2.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

8. Privacy Notices
8.1 The Company will issue privacy notices from time to time, informing the people from whom we collect information about the personal data that we collect and hold relating to them, how they can expect their personal data to be used and for what purposes.

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

9. Individual Rights

9.1 Data subjects have the following rights in relation to their personal data:
9.1.1 to be informed about how, why and on what basis that data is processed (at the Company, we customarily do that via privacy notices);
9.1.2 to obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a subject access request — see CoP D2 about the Company's subject access procedures;
9.1.3 to have data corrected if it is inaccurate or incomplete;
9.1.4 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 (this is sometimes known as 'the right to be forgotten');
9.1.5 to restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful (but the data subject does not want the data to be erased), or where the Company no longer needs the personal data but the data subject requires the data to establish, exercise or defend a legal claim; and
9.1.6 to restrict the processing of personal data temporarily where the data subject does not think it is accurate (and the Company is verifying whether it is accurate), or where the data subject has objected to the processing (and the Company is considering whether the Company's legitimate grounds override the data subject's interests).
9.2 Each of the Company's privacy notices provides details of how these individual rights can be exercised. In most cases, individuals are advised to contact the Company's Data Protection Officer.

10. Individual Obligations

10.1 Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if the information they have provided to the Company changes (for example if one moves to a new house or changes details of the bank or building society account to which they are paid.
10.2 Members of staff may have access to the personal data of other members of staff, students and other clients and suppliers of the Company in the course of their employment or engagement. If so, the Company expects such members of staff to help meet the Company's data protection obligations to those individuals.
10.3 If one has access to Company personal data, they must:
10.3.1 only access the personal data that they have authority to access, and only for authorised purposes;
10.3.2 only allow others to access personal data if they have appropriate authorisation to do so;
10.3.3 keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's Information Security Policy and related Codes of Practice);
10.3.4 not remove personal data, or devices containing personal data (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
10.3.5 not store personal data on local drives or on personal devices that are used for work purposes.
10.4 The Company's Data Protection Officer should be contacted if one is concerned or suspects that one of the following has taken place (or is taking place or likely to take place):
10.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal data, without also one of the conditions in paragraph 5.2.2 above being met;
10.4.2 access to personal data without the proper authorisation;
10.4.3 personal data not kept or deleted securely;

10.4.4 removal of personal data, or devices containing personal data (or which can be used to access it), from the Company's premises without appropriate security measures being in place;
10.4.5 any other breach of this policy or of any of the data protection principles set out in paragraph 3 above.

11. Information Security

11.1 The Company will use appropriate technical and organisational measures in accordance with the Company's Information Security Policy and related Codes of Practice to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
11.1.1 making sure that, where possible, personal data is pseudonymised or encrypted;
11.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
11.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and
11.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
11.2 Where the Company uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. In particular, contracts with external organisations must provide that:
11.2.1 the organisation may act only on the written instructions of the Company;
11.2.2 those processing the data are subject to a duty of confidence;
11.2.3 appropriate measures are taken to ensure the security of processing;
11.2.4 sub-contractors are only engaged with the prior consent of the Company and under a written contract;
11.2.5 the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights in relation to data protection;
11.2.6 the organisation will assist the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
11.2.7 the organisation will delete or return all personal data to the Company as requested at the end of the contract; and
11.2.8 the organisation will provide the Company with whatever information it reasonably needs to ensure that they are both meeting their data protection obligations.
11.3 Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant member of staff must seek approval of its terms by the Company's Data Protection Officer.

12. Storage and Retention of Personal Data

12.1 Personal data (and sensitive personal data) will be kept securely in accordance with the Company's Information Security Policy.
12.2 Personal data (and sensitive personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. The Company's Retention Schedule sets out the relevant retention period, or the criteria that should be used to determine the retention period.
12.3 Where there is any uncertainty with respect to data retention, staff should consult either the Archives or the Company's Data Protection Officer.
12.4 Personal data (and sensitive personal data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

13. Data Breaches
13.1 A data breach may take many different forms, for example:
13.1.1 loss or theft of data or equipment on which personal data is stored;
13.1.2 unauthorised access to or use of personal data either by a member of staff/third party;
13.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;
13.1.4 human error, such as accidental deletion or alteration of data;
13.1.5 unforeseen circumstances, such as a fire or flood;
13.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
13.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.
13.2 If anyone believes personal data held by the Company has been compromised in some way, they MUST report this immediately by completing a notification of data security breach from the DPO.
13.3 The Company will:
13.3.1 investigate any reported actual or suspected data security breach;
13.3.2 where applicable, make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
13.3.3 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

14. International Transfers
14.1 In the event that the Company intends to transfer personal data outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to other countries on the basis that such countries are designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards (e.g. by way of binding corporate rules or standard data protection clauses) or where we obtain the relevant data subjects' explicit consent to such transfers we will:
14.2 Inform data subjects of any envisaged international transfers in the relevant privacy notice.

15. Training
Staff need to be adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

16. Consequences of Failing to Comply
16.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy:
16.1.1 puts at risk the individuals whose personal data is being processed;
16.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and
16.1.3 may, in some circumstances, amount to a criminal offence by the individual.
16.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under the Company'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.
16.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Company's Data Protection Officer.

Review, Induction and Training

- All IG Framework Strategy Policies and Codes of Practice are reviewed and up-date annually or as a result of the application of new regulations or guidelines and are signed-off for publication, application and training at Board level.
- All Staff must evidence their reading and comprehension of all relevant Policies and CoPs as denoted in their Policy Review and Awareness training at induction and yearly thereafter.
- Completion of standard quarterly refresher/clarification training relating to these policies and CoPs is mandatory for all staff.
- Specific training for all staff and managers to ensure they are fully aware of their particular IG responsibilities and duties forms an integral part of the regular in-house monthly training schedule for staff at all levels.
- As well as Privacy Notice awareness training for students information governance and data protection policies are actively promoted and highlighted across the delivery spectrum and embedded in all service transactions.

Should you have any queries, questions, or have knowledge of any incidents or suspected breaches please speak to your Head of Department, or a member of the Senior Management Team, or contact:
Compliance & IT Manager (CIM) - Steve Maddocks
Tel: 01695 558420
Email: steve@sbskills.co.uk
or
Senior Information and Risk Officer and Senior Data Protection Officer
Neil Beaumont, Director
Email: neil@sbskills.co.uk

Manager responsible for this document Stephen Maddocks Compliance Manager
Approved On 21/04/2021
Review Date 21/04/2022

Manager responsible for this document Stephen Maddocks Compliance Manager
Approved On 21/04/2021
Review Date 21/04/2022