SB Skills Solutions
GDPR and Data Processing Policy & Practice (GDPR)

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)
Data Protection Policy (DPP)
Information Security Policy (ISP)
Codes of Practice D1 > D14
CoP D1 Handling Personal Data
CoP D2 Access to Personal Data
CoP D3 Data Asset Register
CoP D4 Impact Assessment
CoP D5 Electronic Messaging
CoP D6 Password Policy
CoP D7 Inspection of Electronic Data
CoP D8 Clear desk & Screen Policy
CoP D9 Archiving
CoP D10 Media Classification
CoP D11 File Control
CoP D12 Shredding and Disposal
CoP D13 Equipment
CoP D14 Auditing
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

GDPR and Data Processing Policy & Practice (GDPR)

GDPR

1.1 General Data Protection Regulation (GDPR)

The EU's General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 are new laws which have replaced the 1998 Data Protection Act. The GDPR was passed in 2016 and all organisations, including SB Skills Solutions, had to become compliant with it by 25 May 2018. The Data Protection Act 2018 came into force and replaced the Data Protection Act 1998 on 23 May 2018. For most organisations, the GDPR is the law to turn to first. However, the Data Protection Act 2018 supplies a lot of the detail about how privacy law will apply to particular sectors and types of activity.

The GDPR only relates to the processing of personal data and has been put into place with the aims of:

- Unifying data privacy laws across the EU.
- Formalising principles of data collection and retention.
- Improving the protection of EU citizens and their data, with new considerations. given to technological advances made since the 1998 Data Protection Act came into place.

1.2 GDPRU Changes

The GDPR places a greater emphasis on the rights of the data subject.

These rights are:

- The right to be informed.
- The right of access.
- The right of rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

According to the new regulation, all personal data must be:

1) Processed lawfully, fairly and in a transparent manner in relation to individuals;

2) Collected for specific, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;

3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4) Accurate and, where necessary, kept up to date; steps should be taken to rectify or erase without delay;

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6) Processed in a manner that ensures appropriate security of the data;

The GDPR also includes an accountability principle which states that we must be able to demonstrate compliance with the above principles.

1.3 Implications

As a result of the GDPR, a number of changes need to be made to the ways in which the SB Skills Solutions holds and processes personal data, and it is important that you are aware of your responsibilities. The main risks of non-compliance are increased fines (the maximum being the greater of 4% global turnover for the preceding financial year or €20 million) and a lack of confidence from the public and other organisations towards the SB Skills Solutions.

1.4 Security

Proper security measures must be applied for all methods of holding or displaying personal data and appropriate measures taken to prevent loss, destruction or corruption of data. The following general advice is given:

- Computers that can access personal data should not be left unattended when logged on and the screen should always be cleared of personal data after use;
- Staff who have contact with personal data must take care that this is kept away from people not entitled to see it;
- Printouts should be stored securely when not in use and shredded when no longer required;
- Passwords should be changed regularly and not disclosed to unauthorised persons. Staff who are processing personal data locally should ensure that USB flash drives containing personal data are securely encrypted, removed from their machine and stored securely when not in use and are erased and reformatted when no longer required, and that personal data held on permanent hard disk have adequate protection, e.g. password access;
- Care should be taken to ensure the security of personal data, in either electronic or paper format, when the data is removed from the Company, e.g. for the purpose of working at home, or for an external meeting.

2. Processing Personal Data

2.1 Definitions

Personal data - Any information relating to an identified or identifiable natural person i.e. 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Information which falls within this definition is always subject to the GDPR.

Sensitive personal data - 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.

This is a special category of personal data subject to additional protections due it its sensitive nature.

For the purposes of providing some student and staff support services (for example, providing reasonable adjustments for disabilities or counselling services), to comply with some legal obligations this type of data is relevant to us.

2.2 Data Processing

As defined by the GDPR, this is a very wide concept. It essentially means anything that is done to, or with, personal data including collecting, storing and deleting it.
Data Controller - The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. SB Skills Solutions is a controller in respect of most of the personal data it processes.
Data Processor - A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a controller.

2.3 Processing Personal Data
Under the GDPR, you are allowed to process personal data only when you have a lawful basis, of which there are six. These are:

1. Contractual necessity - When processing is necessary for the entry into, or performance of, a contract with the data subjects (or at their request prior to the entry into a contract).
2. Compliance with legal obligations. When processing is necessary for compliance with a legal obligation under EU law or the laws of a Member State.
3. Public interest - When 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 SB Skills Solutions.
4. Legitimate interest (unless a public authority) - When processing is necessary for the purposes of legitimate interests pursued by SB Skills Solutions except where overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection.
5. Vital interests - When processing is necessary to protect the 'vital interests' of the data subject or of another natural person.
6. Consent - When processing has been consented to by the data subject. Please see below for clarification on what consent means.

This is relatively unchanged from the previous law, but *consent should now be considered last* as a higher standard of consent is required under the GDPR.

2.4 Consent
Consent needs to be:

- Specific;
- Informed;
- Freely given (a performance of a contract must not be made conditional on the data subject consenting to processing activities that are not necessary for the performance of that contract);
- Able to be evidenced;
- Able to be withdrawn;
- Opt-in rather than opt-out;
- Provided by an appropriate method;
- Distinguishable from other matters;

2.5 Processing Sensitive Personal Data

You can process sensitive personal data when, in addition to having fulfilled one of the previously given lawful bases for processing, one of the following conditions is also satisfied:

1. Legal claims:
   The processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.
2. Employment or social security laws:
   The processing is necessary in the context of employment law, or laws relating to social security and social protection.
3. Substantial public interest:
   The processing is necessary for reasons of substantial public interest and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects.
4. Vital interests:
   The processing is necessary to protect vital interests of the data subject (or another person) where the data subject is incapable of giving consent.
5. Medical diagnosis and treatment:
   The processing is necessary for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services.
6. Charity or not for profit bodies with respect to their own members'
   The processing is in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes.
7. Public health:
   The processing is necessary for reasons of public interest in the area of public health (e.g. ensuring the safety of medicinal products).
8. Data manifestly made public by the data subject:
   The processing relates to personal data which have been manifestly made public by the data subject.
9. Archiving in the public interest, for historical, scientific, research or statistical purposes.
   The processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.
10. Explicit consent - The processing is carried out with the explicit consent of the data subject.

2.6 Information Rights

You should provide data subjects with information about their rights and your responsibilities regarding the processing of their personal data. This will typically be in the form of a **Privacy Notice** for Students or Staff and must be in a concise, transparent, intelligible and easily accessible form. Any information provided to children must be especially plain and clear.
This should be done at the time the data is obtained or at a minimum, within a reasonable time (not exceeding one month) after collecting the data.
You can contact the SIRO/DPO if you require assistance.
If you are proposing to use data already collected for a purpose that data subjects were not told about when they gave their data (the further processing of data): you should contact the SIRO/DPO.

You and the Data Protection Officer will need to consider if such further processing is compatible with the original purpose and is therefore lawful. We will also have to consider if data subjects ought to be informed again of the proposed further processing of their data.

3. Sharing Personal Data

3.1 Data Sharing

Data sharing in this context refers to the disclosure of personal data by the Company to anyone outside the Company i.e. sharing with third parties (e.g. to a third party organisation, an individual consultant, a training collaborator, a commercial partner or a service provider) whether as a separate data controller or as a data processor.
Note that one department using personal data collated by another department within the Company is not data sharing under this guidance. Considerations in such cases would be about whether the data is being used within Company for the purpose for which it was collected and as per the information given to the individuals whose data that is.

3.2 Sharing Personal Data with Third Parties

The Company may be able to share personal data with third parties, but only under certain conditions. These are where:

- Sharing is necessary for a legitimate purpose;
- It is not illegal otherwise e.g. because of confidentiality provisions;
- We have told people, or are going to tell them before the sharing, that we will be sharing their data;
- We are going to share the minimum that is necessary for the purpose of the sharing;
- We enter into data sharing/processing documentation with the third party, see below.

3.3 Mandatory Data Processing Agreements

A data processing agreement is mandatory where a controller wishes to appoint a processor to process personal data on behalf of the controller. In such circumstances, both the controller and the processor are responsible to ensure that such an agreement is put into place.
As a controller the Company must only use processors that guarantee compliance with the GDPR and the Company is obliged to appoint such processors in the form of a binding agreement in writing – typically, this takes the form of a data processing agreement, but it can also take the form of data processing clauses or a data processing addendum inserted into the agreement for services with the processor e.g. sub-contracting.
3.3.1 Data sharing agreements are not mandatory but are a good practice to put into place so that it is beyond doubt what each party's responsibilities and obligations are, what security measures will be in place when the data is shared and who the relevant contacts are at each organisations. There may be instances where the parties sharing personal data are each a controller for most of the data and a processor for some of the data of the other party. In this scenario, a data processing agreement is necessary.
3.3.2 Data Processing Agreements must say that the processor must:

- Only act on the controller's documented instructions;
- Impose confidentiality obligations on all personnel who process the relevant data;

- Abide by the rules regarding appointment of sub-processors and the rules about transfers of personal data outside the EEA;
- Implement measures to assist the controller in complying with the rights of data subjects;
- Assist the controller in obtaining approval from data protection authorities (the ICO in the UK) where required;
- At the controller's election, either return or destroy the personal data at the end of the relationship (except as required by EU or member state law);
- Ensure the security of the personal data it processes;
- Provide the controller with all information necessary to demonstrate compliance with the GDPR and allow for and contribute to audits (including inspections) conducted by the controller or another auditor mandated by the controller;
- Assist the controller in ensuring compliance with the controller's security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and, when necessary, consultation with the data protection authorities, taking into account the nature of processing and the information available to the processor;
- Inform the controller if an instruction from the controller infringes EU data protection law

Data Processing Agreements must also contain the following details (which will be specific to each individual case):

- The name and contact details of the processor and the controller and, where applicable, of their data protection officers;
- The subject matter, nature and purpose, or purposes, of the data processing;
- The duration of the processing;
- The types of personal data to be processed and categories of data subjects;
- Where possible, a general description of the technical and organisational security measures protecting the personal data

Indemnities, caps of liability in the event of breach of data processing obligations and mandatory insurance may also be found in some Data Processing Agreements but they are optional.

For more information please see the ICO - Data Sharing Code of Practice and the ICO - Data Sharing Checklist.

3.4 International Data Transfers

Data can be transferred to countries outside of the EEA when the following occurs:

- If data is transferred to a country with an Adequacy Decision from the EU Commission (this remains unchanged even in the event of a no deal Brexit);
- When standard EU model clauses are signed by the recipient (this remains unchanged even in the event of a no deal Brexit);
- If, to the US, the recipient has self-certified under the EU-US Privacy Shield (or the recipient signs the standard EU model clauses) (in the event of a no deal Brexit, the recipient in the US has to amend its EU-US Privacy Shield certification so as to refer to the UK expressly (in addition to the EU) – if they do not do that, the Company cannot rely on the EU-US Privacy Shield as the basis for transferring data to the US recipient and the US recipient will most likely need to sign up to the EU model clauses instead);
- When binding corporate rules are in place (rarely encountered in practice by the Company) (this remains unchanged even in the event of a no deal Brexit);

- Explicit consent is given from the data subject – but this is not an option where the Company is exercising public functions (this remains unchanged even in the event of a no deal Brexit);
- It is necessary for the performance of a contract – but this is not an option where the Company is exercising its public functions or has simply chosen to structure its activities in that manner (this remains unchanged even in the event of a no deal Brexit);

If personal data will only be in transit through a non-EEA country and therefore not accessible outside the EEA, this does not count as a transfer outside the EEA.
You should always consider whether a transfer of personal data is necessary in the first place. If you conclude that it is, please contact the Data Protection Officer, the Deputy Data Protection Officer or the legal team for advice on how to arrange and document the transfer.

4. Data Retention

Personal data should not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.
In some cases the retention period may be determined by law, but in others it is a matter of best practice.
The Company's retention periods for different categories of records are set out in the Company's retention schedule. For further detailed advice on document retention please contact the SIRO/DPO.

5. Data Protection Impact Assessments

Under data protection legislation, where a new processing activity is proposed and results in a high degree of risk for data subjects, staff must first conduct a data protection impact assessment (DPIA). You may see this occasionally referred to as a data privacy impact assessment. The aim of a DPIA is to systematically analyse the processing and help you to identify and minimise data protection risks.
A DPIA is a process you can use to analyse your data processing. It must:

- Describe the processing and your purposes;
- Assess necessity and proportionality;
- Identify and assess risks to individuals; and
- Identify any measures to mitigate those risks and protect the data.

DPIA's are necessary whenever a type of processing is likely to result in high risk for data subjects. This means that although the actual level of risk has not been assessed yet, you need to screen for factors which point to the potential for a widespread or serious impact on individuals.
In particular, the GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

It is good practice to carry out a DPIA for any major project involving the use of personal data. If you identify a high risk which you cannot mitigate, please consult the SIRO/DPO.
(See CoP D4)

6.Reporting a Data Breach

A personal data breach is a breach in security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
This includes breaches as a result of both accidental and deliberate causes.
Breaches might include:

- If you have sent information which is considered personal data or sensitive personal data to the wrong recipient, or if you have received such information and it was not intended for you.
- If your work or personal mobile devices, tablets or laptops have been lost or stolen and personal data is stored on those devices.
- If your work or personal devices have become vulnerable to a virus or malware.
- If you have reason to believe another individual has had access to information they should not have – either by entering a private office or accessing an unlocked device.
- If you become aware that personal data belonging to the Company has been the subject of a breach of security while in the hands of any provider of services to the Company.

Under the GDPR, the Company must report certain types of personal data breaches to the ICO without undue delay, and within 72 hours of becoming aware of it. What this means is that if you become aware of or suspect a data breach, you must report it as soon as possible (within 72 hours of becoming aware of it) to the SIRO/DPO.

The SIRO/DPO will then consider and decide whether the ICO and data subjects need to be notified – where the breach is at a high risk of adversely affecting individuals' rights and freedoms. If the Company decides that the breach does not need to be reported, justification may be required. Therefore, the decision process must be documented.
It is important that you report a breach as soon as possible so we can contain and control any further damage. We will need to contact you as part of our investigation, so please ensure you provide your contact details. If the data breach concerns your team or department, you and your colleagues may also be asked to assist with notifying affected individuals (where that is necessary) and to help prepare a notification to the Information Commissioner (where notification is required).

7.Subject Access Requests

The EU General Data Protection Regulation (GDPR) grants subjects or individuals the right to access your personal data held by SB Skills Solutions. These requests are known as subject access requests and in accordance with the GDPR, we will provide you confirmation that we are processing your personal data, provide you information pertaining to the processing of your personal data and provide you a copy of the personal data we hold.
Subject access requests can be submitted in writing or made verbally (subject to proof of identification) to the SIRO/DPO.
We expect to respond to your request within one week of receipt of your subject access request and proof of identity. In some cases (where requests are complex or numerous) we may take up to a further4 weeks; we will let you know where this may be the case.

8.Marketing

Where the Company is involved in direct marketing to individuals we need to comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") in addition to the GDPR. PECR regulate marketing by electronic means such as email, phone, text or fax, and also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches.

There are PECR rules that apply to business-to-business marketing but they are different from the rules that apply to marketing to individuals (which includes sole traders and some partnerships). In general, the rules on marketing to companies are not as strict.

There are different rules for live calls, automated calls, faxes, and electronic mail (this includes emails or texts). Most of the rules in PECR only apply to unsolicited marketing messages. They do not restrict solicited marketing. Put simply, a solicited message is one that is actively requested. So if someone specifically asks you to send them some information, you can do so without worrying about PECR (although you must still say who you are, display your number when making calls, and provide a contact address).

An unsolicited message is any message that has not been specifically requested. So even if the customer has 'opted in' to receiving marketing from you, it still counts as unsolicited marketing. An opt-in means the customer agrees to future messages (and is likely to mean that the marketing complies with PECR). But this is not the same as someone specifically contacting you to ask for particular information. This does not make all unsolicited marketing unlawful. You can still send unsolicited marketing messages – *as long as you comply with PECR.*

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

Version History Version/Status

Comments		
1.1/Approved	June 2018	Approved by Board of Directors
1.2/Approved	January 2019	Approved by Board of Directors
1.3/Approved	January 2020	Approved by Board of Directors
1.4/Approved	January 2021	Approved by Board of Directors

Review Date January 2022