SB Skills Solutions
Codes of Practice

This Policy should be read in conjunction with other Data Management and Information Governance Policies and related Codes of Practice (CoPs) including:
Information and Data Governance Framework (IDGF)
Data Protection Policy (DPP)
GDPR & Data Processing Policy & Practice (GDPR)
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 Manager - 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

Code of practice 1 - Handling of Personal Data

1.Introduction

This Code of Practice, drawn up in association with the SB Kills Solutions's Data Protection and GDPR Policies, relates to the collection, holding and disclosure of data relating to individuals. The Code provides best practice for staff and students of SB Skills Solutions and other authorised persons who collect, process, disclose or have access to personal data in whatever medium that data is held. In the terms of the General Data Protection Regulation (GDPR) "processing" covers all aspects of handling personal data, including obtaining, recording, holding, retrieving, collating, disclosure, erasure and destruction of data.

2. Keeping Records of Processing Activities

SB Skills Solutions has an obligation to keep records of its data processing activities. This replaced the obligation to notify the Information Commissioner of what personal data SB Skills Solutions processes. The records that SB Skills Solutions must keep include:

- the contact details of the Data Protection Officer;
- the purposes of the processing;
- the categories of data subjects and personal data processed;
- the categories of recipients with whom the data may be shared;
- information regarding Cross-Border Data Transfers;
- the applicable data retention periods; and
- a description of the security measures implemented in respect of the processed data.

Upon request, these records must be disclosed to the Information Commissioner.

To help SB Skills Solutions comply with its record keeping obligations, all Company information assets (including those that contain personal data) must be registered in the Company's Information Asset Register and must have an identified Information Asset Owner who (among other things) is responsible for updating the record as and when necessary (see CoP D3).

3. Collecting and Processing of Personal Data

3.1 Collection and processing of Personal Data must comply with the data protection principles. Personal data users have a duty to make sure that they comply with the GDPR and handle personal data in accordance with the data protection principles. These are set out in SB Skills Solutions's Data Protection and GDPR & Data processing Policy and Practice. In summary these state that SB Skills Solutions will:

- process personal data lawfully, fairly and in a transparent manner;
- 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;
- only process the personal data that is adequate, relevant and necessary for the relevant purposes;
- keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;
- 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;
- 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;
- demonstrate compliance with the above data protection principles.

3.2 Personal data is “any information relating to an identified or identifiable natural person (referred to as a “data subject”); an identifiable natural 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, 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. So, some obviously personal data are name, contact details (post, phone, e-mail etc.), relationship, educational and financial details. Less obviously personal data are IP addresses and device IDs, pseudonymous data (e.g. hashed or encrypted data).
3.3 In addition, personal data has a sub-set known as ‘sensitive personal data’ or ‘special categories of data’. These are data relating to a data subject’s:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of unique identification
- health
- sex life or sexual orientation

Sensitive personal data has a higher standard of protection than other personal data.
3.4 The data protection law also treats criminal data with a higher degree of care than other personal data.
3.5 The term "processing" is broad. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting those data). This definition is significant because it clarifies the fact that the GDPR is likely to apply wherever an organisation does anything that involves or affects personal data.
3.6 Processing ‘standard’ personal data:
3.6.1 We must have one of six prescribed lawful bases for processing personal data. Seeking consent from the individuals whose data they are is one basis for processing but should be considered only where there is no more suitable legal basis for the processing.
3.6.2 The six lawful basis are:

- processing is permitted if it is necessary for the entry into, or performance of, a contract with the data subject or in order to take steps at his or her request prior to the entry into a contract (in short, there is contractual necessity);
- processing is permitted if it is necessary for compliance with a legal obligation under EU law or the laws of a Member State (in short, where SB Skills Solutions has to comply with a UK or EU law legal obligation);
- processing is permitted if it is necessary in order to protect the vital interests of the data subject or of another natural person (in short, to protect vital interests);
- processing is permitted if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller under UK or EU/ EU Member States law (in short, the public interest basis;
- processing is permitted if it is necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection, particularly where the data subject is a child (in short, the legitimate interest basis).processing is permitted if the data subject has consented to the processing (i.e. with consent).

3.6.3 Consent must be unambiguous, verifiable (we ought to document proof of consent), distinguishable from other matters, easy to withdraw, (generally) must not be conditioned on access to a service. Silence, inactivity and pre-ticked boxes do not amount to consent.
Not only is the standard of valid consent under the GDPR high but if we seek consent to the processing of personal data, the individuals who have consented will also be able to exercise the right to erasure and the right to portability more.
3.7 Processing sensitive data
The GDPR imposes a number of additional restrictions and conditions on data controllers who want to record and process sensitive personal data. SB Skills Solutions can process sensitive personal data when (in addition to having a lawful basis as explained above) for processing any personal data, we can also satisfy one of ten additional grounds which are as follows:

- Legal claims;
- It is necessary in the context of employment law, or laws relating to social security and social protection;
- Reasons of substantial public interest;
- To protect vital interests;
- Medical diagnosis and treatment (undertaken by health professionals, including assessing the working capacity of employees);
- Charity or not-for-profit bodies with respect to their own members;
- Public health;
- Data manifestly made public by the data subject;
- For archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards;
- Obtain explicit consent;

We should document our analysis on this.
3.8 Staff, and to some extent students, collect both ‘standard’ and sensitive personal data on employees, students and other individuals.
3.9 Most personal data which is collected on a day-to-day basis will be "standard", i.e. for general administrative purposes, and will cover categories such as:

- General personal details such as name, address, date of birth and next of kin;
- Details about class attendance, course-work marks and grades and associated comments;
- Notes of personal supervision, including matters about behaviour and discipline;
- Management of student clubs and societies.

3.10 A data protection impact assessment (in short, DPIA), must be conducted:

- where there is “high risk” to data subject rights and freedoms;
- prior to processing;
- in consultation with the Data Protection Officer.

A DPIA is always required where there will be:

- automated decision with legal / significant effect;
- large scale sensitive data processing;
- large scale monitoring of public areas.

Consultation with the Information Commissioner is required if high risks cannot be mitigated.
3.11 Data Subjects must be informed of the purposes for which data is being collected at the point of collection. SB Skills Solutions informs students and prospective students of how it uses their personal data in its Privacy Notices for Students and **Privacy Notice for Staff &**

Volunteers. Any additional processing which is done and which is not explained and provided for in these notices or which applies to other categories of Data Subjects will require careful analysis as to the lawful basis of processing, data protection impact assessment and its own privacy notice to inform the relevant Data Subjects of the proposed processing.
3.12 All personal data must be held securely in accordance with the Company's Information Security Policy. All persons having access to such data shall treat it as confidential and shall not communicate it to other persons or bodies except in accordance with this Code of Practice.
3.13 Before processing any personal data, members of SB Skills Solutions and other authorised individuals should study the checklist for processing data set out in the **Appendix to this Code.**
3.14 Where any of the data protection principles are not followed data users may find themselves subject to Company disciplinary procedures. Also, SB Skills Solutions may be investigated and fined by the Information Commissioner and may be liable to pay compensation to any affected individuals
3.15 Disclosure of personal data to third parties
3.15.1 No data relating to a particular student, member of staff or other individual acquired in the course of an individual's duties should be disclosed to anyone (including other students or staff) unless:

- required for normal training, administrative or pastoral purposes of Company business, or
- the individual concerned has given permission, or
- they are required to do so in the discharge of regulatory functions or required by legislation, or
- in the case where, even though prior consent has not been given, disclosure is deemed to be needed to protect the vital interests of the Data Subject or it is required for the prevention or detection of crime or the apprehension or prosecution of offenders, or
- in certain limited cases and subject to certain conditions and safeguards, it is used for legitimate statistical purposes.

3.15.2 In many cases, sharing of personal data is relevant to Company, when the Company appoints another organisation to process data on behalf of SB Skills Solutions, or where an organisation provides services to SB Skills Solutions, that require that organisation to have access to Company-owned personal data or to systems holding Company-owned personal data. This is known as appointing a processor.
3.15.3 SB Skills Solutions must only use processors that guarantee compliance with the GDPR. SB Skills Solutions must appoint the processor in the form of a binding agreement in writing (such as a data processing agreement or a services agreement with appropriate data processing clauses), which states that the processor must only act on the Company's documented instructions. The agreement must also contain a number of other provisions prescribed by the GDPR.
3.15.4 Before sharing any data (personal or other) staff should consider the following key questions:

- Do you have the legal power or ability to share the data in question?
- Will the proposed data sharing involve sharing of "standard" personal data and sensitive personal data and, if so, would the sharing be fair, transparent and in line with the rights and expectations of the people whose information is being shared? Check what people have been told in the relevant privacy notice about data sharing.
- Is there any specific statutory prohibition on sharing the data in question?

- Are there any copyright restrictions?
- Is there a duty of confidence (express or implied by the content of the information or because it was collected in circumstances where confidentiality was expected e.g. medical or banking information)?
- If a decision is ultimately taken to share data with another organisation or person, will a data processing or data sharing agreement be signed or will the services agreement include data processing/sharing provisions? This is a requirement.

3.16 Transfer of data overseas

3.16.1 The transfer of personal data to recipients outside the EEA is generally prohibited unless:

- the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;
- the data exporter puts in place appropriate safeguards; or
- an exemption applies such as the transfer is required for the performance of a contract between a data subject and a data controller, or for taking steps at the request of a data subject with a view to entering into such a contract, or where specific and informed consent of the data subject has been obtained for effecting such a transfer.

Where staff contemplate transferring personal data outside the EEA, they should discuss the proposal with the Data Protection Officer to establish if there is a lawful basis for such transfer.

3.16.2 Posting personal data to the World Wide Web constitutes transfer of data worldwide. A third party accessing Company-owned personal data from outside the EEA would also constitute a transfer of data outside the EEA. Using a cloud services provider with servers outside the EEA would also constitute a transfer of data outside the EEA. However, if data is only in transit through a non-EEA country (and is not accessible) this will not constitute a transfer outside the EEA.

3.16.3 Subject to taking appropriate security measures, as set out in 3.17 below, personal data may be transferred to countries in the European Economic Area (EEA) without further restriction.

3.16.4 Proper records must be kept justifying any decision made about such exempted transfers, or clear evidence can be demonstrated showing the Data Subject had given consent to the transfer, having been suitably informed.

3.16.5 In the absence of a sponsorship arrangement between SB Skills Solutions and an external body in respect of a particular student, personal data should not be disclosed in response to a request from non-EEA governments, agencies or organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas without specific informed consent of the Data Subject(s) concerned, nor should such data be disclosed to such bodies for the purposes of determining liability to attend National Service without such consent.

3.17 Security

3.17.1 Proper security measures must be applied to all methods of holding or displaying personal data and appropriate measures taken to prevent loss, destruction or corruption of data. For fuller details on security measures see the Information Security Policies, and associated Codes of Practice.

3.17.2 Staff, students and authorised third parties are not permitted to remove from SB Skills Solutions personal data with the intention of processing this information elsewhere, unless such use is authorised by the data owner and that authorisation recorded. Removing data in this way

must not compromise the standards of security operating within the Company, and the data protection principles should be observed at all times.

Appendix - checklist for processing of personal data

- Do you really need to record the information?
- Which is your legal basis for processing the information (one of six bases)?
- Is the information "standard" or is it "sensitive"?
- If it is sensitive information, do you satisfy one of the ten additional conditions to be able to process the information?
- If you are going to rely on consent to process “standard” personal data or “sensitive” personal data, are you able to obtain valid consent?
- Has the data subject been told how the data will be processed?
- Are you authorised within Company to collect/store/process the data?
- If yes, are there mechanisms in place to check the accuracy of the data?
- Is it clear who else has a right to access/process these data?
- Do you have mechanisms in place to ensure that the data are kept securely whether held electronically or in a relevant filing system?
- Are you clear as to how long you may retain these data?
- Do you have procedures in place to ensure that the data is kept up to date?
- Do you have procedures in place to remove these data securely when it is no longer needed?
- Do you have procedures in place to remove these data where a data subject exercises their right for it not to be processed;
- Has a data protection impact assessment been carried out either because it is mandatory or as best practice?

Code of Practice 2
Access to Personal Data

1.Introduction

1.1 This Code of Practice, drawn up in association with the Company’s Data Protection and GDPR Policies, relates to the access by individuals (data subjects) to data relating to themselves. The Code provides procedures for past and present staff and students of the Company and other third parties to access the personal data held on them in Company systems in whatever medium that data is held, and for dealing with requests for such subject access.

2.Access to personal information

2.1 The Company respects the right of individuals (also known as subject access rights or SAR) to obtain the following:

- confirmation of whether, and where, the Company is processing their personal data;
- information about the purposes of the processing;
- information about the categories of data being processed;

- information about the categories of recipients with whom the data may be shared;
- information about the period for which the data will be stored (or the criteria used to determine that period);
- information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;
- information about the existence of the right to complain to the Information Commissioner;
- where the data was not collected from the data subject, information as to the source of the data; and
- information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects.

Additionally, the Company respects the right of data subjects to request a copy of the personal data being processed.

2.2 In certain circumstances, an exemption to the GDPR requirement to grant access to personal data might apply. Such exemptions include:

- where disclosure would simultaneously disclose data about another person (unless that person consents to the disclosure);
- third party references and examination marks (see paragraphs 3 and 4 below for further information)

2.3 Any data subject wishing to gain access to personal data held about them may do so by the submission of a request to the Data Protection Officer (DPO). The Company may also require proof of identity to ensure the individual making the request is the individual to whom the personal data pertains. Where a request is submitted on the behalf of another individual (such as by an individual's legal representative), then signed authorisation will be required from the data subject. The Company aims to comply with requests for access to personal data as quickly as possible but will ensure that it is provided within one month of receipt of the application form.

2.4 Subject access requests submitted to the Company are processed by the Company's DPO in liaison with Company departments and/or staff members (as is appropriate in each case).

3. Confidential References

3.1 References issued by or on behalf of the Company

Confidential references issued by the Company or an individual member of it in the performance of Company duties are exempt from subject access where these references relate to:

- education, training or employment of the data subject;
- appointment of the data subject to any office;
- provision by the data subject of any service.

3.2 References Received by the Company

3.2.1 Confidential references received by the Company are exempt from the right of access by the data subject to whom they refer provided that such references have been written "In Confidence" and clearly state this. However, this exemption from disclosure to the data subject may not be possible to rely on in all circumstances – and the Company may decide in any event that it is reasonable to disclose the reference (possibly, after anonymising it e.g. to remove the identity of the referee or where the referee has given his/her consent).

3.2.2 Where, in response to a subject access request, the Company declines to disclose a reference received in confidence from a referee, it will supply clear reasons in writing for doing

so. Members of the Company may not refuse to disclose references received in confidence from referees without providing, in writing, the reasons for the refusal.

4. Examinations

4.1 In accordance with the GDPR, information recorded on their scripts by students during an examination are exempt from subject access. However, students are entitled to information about their marks for both coursework and examinations. In accordance with the GDPR, this will be made available either 5 months from the day on which the Data Protection Officer received the request and any fee which may apply, or one month from the announcement of the examination results. The Company, however, reserves the right to withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the Company.

4.2 A data subject has a right to request a copy or summary "in an intelligible form" of any comments made on an examination script by an examiner, within the same periods as laid down for access to examination marks.

4.3 A data subject has a right of access to those parts of Minutes of Examination Boards or special circumstance committees which contain discussion about themselves where they are named or referred to by identifiers from which the candidate may be identified unless the data cannot be disclosed without additionally disclosing personal data about a third party.

Code of Practice 3 - Information Asset Register

1. Introduction

This Code of Practice is to be read in conjunction with the Information Security Policy, Data Protection Policy, GDPR and Data processing Policy and Practice, and wider Information Governance Policy Framework.

It governs the use of the Information Asset Register (also referred to as the “IAR”), and the requirement for Information Asset Owners (also referred to as “IAOs”) to register, and maintain the registration of, their information assets in the IAR.

2. Key Terms

The following key terms are of particular relevance in this Code of Practice:

Information Asset

Information which satisfies each of the following criteria will qualify as an “information asset” for the purposes of asset registration and must have an entry in the Company Information Asset Register

- the information contains personal data and/or sensitive personal data relating to an identifiable or potentially identifiable natural living person or persons;
- the information is intended to be kept for more than 6 months or may be kept for less than 6 months but could still represent a significant risk to the Company if a data breach occurred; and
- each record within the information, whether in digital or physical format, will have shared purpose, risk profile, and risk mitigation measures that make the information a logical collection of data.

There must be a lawful basis within the meaning of the General Data Protection Regulation (GDPR) for the processing of any personal data and/or sensitive personal data within each information asset. Collection of personal data or sensitive personal data without a lawful basis for the collection is not permitted.
The following are some examples of information assets:

- a database of staff personal details or a database of students' details;
- a database (in physical or electronic format) containing newsletter subscribers' contacts details;
- Personal Review and Development Plans (PRDPs) are collectively a single information asset but managed across multiple departments. They should be subject to the same rules and owned, collectively, by an Information Asset Owner from Human Resources.

Information Asset Owner

IAOs are senior/responsible individuals working in a relevant business area. Their role is to understand what information is held within their business area, what is added and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information that information is used within the law and in line with the Company's objects and provide written input to the Company's Senior Information Risk Owner annually on the security and use of their information assets.
An IAO will be responsible for an information asset in terms of:

- identifying risks associated with the information asset;
- managing and operating the asset in compliance with policies and standards; and
- ensuring controls implemented manage all risks appropriately.

More details on the role of the IAO can be found at Appendix B to this Code of Practice.

Information Asset Administrator

Information Asset Administrators (also referred to as "IAAs") work on a day-to-day basis with information contained in an information asset. They have day-to-day responsibility for the asset, and make sure that policies and procedures are applied and adhered to by staff and can recognise actual or potential security incidents relating to their information asset. They are responsible for reporting such incidents to their IAO and consulting the IAO on incident management. The role is flexible and is expected to be performed in addition to existing duties. It is possible that the IAO of an information asset is also the IAA of that asset.

3. Use of the Information Asset Register

3.1The IAR will be the single point of reference for all information assets with data protection significance held across the Company. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the personal data within an information asset transmitted, stored or otherwise processed will have compliance and reputational consequences for the Company. The IAR is therefore a tool that is envisaged to assist the Company's data protection compliance processes.
3.2 Information Asset Owners must:

- when creating an asset record, ensure that all information asset attributes are completed, seeking advice from IT, or the Data Protection Officer where necessary;
- make sure the asset record is up-to-date and comprehensive – Appendix A to this Code of Practice indicates the type of information that will need to be input into the system;
- ensure that access records are maintained on the IAR;
- identify all interested parties in the proper-management of their asset;
- upload documents where required (e.g. training records, local policies);

- when DPIA functionality is enabled conduct the regular DPIA review. They should attend IAO training sessions to ensure they have a good understanding of the IAR and update themselves on any legislative and policy developments relevant to information governance.

3.3 The IAR:

- is cloud based and can be accessed via the Company's Single Sign On facility:
- each information asset should have an allocated IAR and an IAA. The owner and administrator can, if necessary, be the same person;
- the system only permits a single IAO to be recorded against information assets. An IAO can own more than one information asset;
- can provide reports on ownership, risk and other metrics.

3.4 Ongoing viability:

- If an IAO leaves the Company they should ensure they hand over their IAO responsibilities ahead of their departure, ensuring their successor is able to access the IAR.
- Where no Information Asset Owner exists, IT Governance will assume the role of IAO pending the allocation to an appropriate candidate in the appropriate faculty or department.
- The product is supported by IT Service Desk. Calls should be logged in the normal manner where they will be triaged. The system is supported internally by IT.

Appendix A: Structure of Information Asset Register – Field Explanation

- Information Asset Owner

Who is responsible for the information stored in this information asset, and is the point of contact for queries about this information asset?

- Information Asset Administrator

The role of the information asset administrator is defined in the Company's Information Governance Policy Framework document and can be summarised as the most senior day-to-day user of the asset.

- Name of the Information Asset

A unique name for the information asset.

- Description of the Information Asset

Please provide a brief description of the information asset. Where possible, please provide a brief overview of the kinds of information held.

- Status - Temporary, Approved or Inactive.
- Classification- Does the asset contain sensitive data? What are the risks associated with this data and how are they mitigated?
  Sensitive data includes:
  1. Commercially sensitive administration.
  2. Sensitive personal data (also known as special categories of personal data), as defined in the General Data Protection Regulation. This encompasses personal data related to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of unique identification, health, sex life or sexual orientation.

3. Personal financial data.
4. Personal data, not included in the categories above, but where accidental release of the data is likely to be detrimental or distressing to the individuals the data is about.

- Media Type - Electronic, Manual or Both.
- Lawful Basis - What is the lawful basis used to justify the holding and processing of this data. For personal data this needs to be a valid reason under either the GDPR or the Data Protection Bill.
- Business Criticality - A ranking of how essential the information is, and the disruption that could be caused by its loss or compromise.
- Location - Where is this data physically stored? For example, on a local computer, in the central Company system, on an offsite server.
- Created By - Who is entering this record into the Information Asset Register?
- Retention Schedule - How long is the information kept for, and what is the process for identifying information that is no longer needed and securely destroying it? You may wish to consult the Company's retention schedule for guidance on how long certain records should be retained.
- Earliest Record - Date of the oldest record which should not be within the range of (present day minus retention period).
- Latest Record - Date of the last record for information assets which are no longer to be updated.

Information Asset Owners will also need to have an understanding of, and enter, the following information into the Information Asset Register:

- Responsible Department Which department is accountable for this information asset? (Most likely the department of the IAO)
- Who has access to this asset? Please briefly describe the group of people who have access to this information asset – e.g. staff in a particular team, all staff in a Department. It is particularly important to note if any non-Company employees have access to the data held on this information asset.
- How is the information kept secure? Please provide a brief description of how the information is kept secure (e.g. is access password protected, are paper records containing sensitive data kept in a locked filing cabinet and how are the keys stored?) NB. Do not write down your password or the location of your keys here!
- Back-up, Resilience and Disaster Recovery arrangements What arrangements are in place to recover data and/or maintain functionality in case of loss or corruption of data / system(s), including disaster level events?

Appendix B: Role of Information Asset Owner

The role of the Information Assert Owner (IAO) is a vital part of protecting and maximising the efficient use of information in Company. The main purpose of the role is to understand and address risks to the information they 'own', usually as part of their management of the service. It also provides assurance to the Senior Information Risk Owner (SIRO) on the security and use of these assets.

Specific Responsibilities:

The Company has adopted the concept of an Information Asset Owner (IAO) as defined by the Cabinet Office in respect of Information Asset Owners in UK government departments; this is as follows:

"Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process."
Specifically, this means that IAOs:

- lead and foster a culture that values, protects and uses information for the public good;
- undertake and pass information governance training and maintain a high degree of awareness of the legal framework;
- understand and address risks to the asset and provide assurance to the SIRO;
- maintain understanding of 'owned' assets and how they are used;
- observe compliance with the provisions of the General Data Protection Regulation in respect of personal data;
- approve information transfers only to achieve business purposes avoiding unnecessary data moves and duplication;
- approve and oversee the disposal mechanism of the information when it is no longer needed;
- know what information the asset holds and who has access to the asset and why; define the process and approval mechanism of how access is authorised and oversee that these requests are logged;
- abide by and enforce compliance with the Information Security Policy in relation to the information asset they own;
- undertake regular reviews on the information risks associated with the asset as described in this Code of Practice;
- employ IT's Change Management process for any changes made to information assets managed by IT.

Code of Practice 4
Data Privacy Impact Assessment

1. Introduction
1.1 This Code of Practice is to be read in conjunction with the Information Security Policy, Data Protection Policy, GDPR & Data Processing Policy and Practice, and wider Information and Data Governance Policy Framework.
1.2 It governs the completion of the Data Privacy Impact Assessment, whether it be on an 'as required' basis (within IT project management methodology or wider business as usual application), or for Information Asset Owners to complete as part of their annual review of their information assets.

2. Data Privacy Impact Assessment
2.1 Information Asset Owners are required to manage their information assets in accordance with the responsibilities outlined in the Information and Data Governance Policy Framework.
2.2 Information Asset Owners should be prepared to undertake a review at the very least annually, and certainly when there is a significant change in the asset, the hosting of the asset,

or significant legislative or policy changes which impact on the personal data held within.
2.3 Information Asset Owners must ensure that the security of their asset meets the requirements of the Company's Information Security Policy, such that:
• All users are properly authorised before they may access the information.
• Appropriate levels of security are adopted according to the value and/or sensitivity of the information.
• They must report any incident which results in, or has the potential to result in, a breach of security to the IT's Service Desk immediately. Concerned individuals may contact any HOD or member of SMT or the Compliance Manager or SIRO/DPO direct.
• They must carry out a Data Privacy Impact Assessment of their assets as part of the annual information asset register review.
2.3.1 Every Information Asset Owner agrees to take at all times every reasonable care to ensure that all material held on information assets they own:
• are lawful.
• comply with "Conditions of Use of IT Resources (Acceptable Use Policy)" in the Company's Information Security Policy.
• do not contain links to unlawful material or material that does not comply with the Company Conditions of Use of (IT) Facilities.
• do not, purport to promote or comment, in the Company's name, upon any commercial goods, products or services, unless approved by a HOD.
• do not purport to promote or comment upon any company, partnership, consortium or consultancy or any "private" activity of the Information Asset Owner or any other person, unless approved by a HOD.
2.3.2 Any individually owned information on Company information assets:
• Should not display logo, logotype, page layout or format belonging to Company.
• The material must be relevant to or associated with the information owner's authorisation to use Company IT facilities.
• These regulations and the appearance of individually owned information, howsoever referenced, do not imply in any way whatsoever that the Company approves or endorses individually owned information or takes any responsibility for individually owned information itself or any material or opinions contained therein. An approved disclaimer must appear on all individually owned information indicating that this information is not formally published by the Company.
2.4 All staff at the Company are responsible for following good information security practice to ensure information held by the Company is properly protected, irrespective of the format in which it is held. Heads of Departments (HODs) are expected to have oversight of the information security practice in their department, as part of their management responsibilities. As part of this process, HODs are required to review assets within their department, and ensure that the Company's Information Asset Register represents an accurate picture of all managed assets (CoP D3).
2.5 The asset register also allows IT Security and IT Governance to identify specific information assets where departments may benefit from specialised IT support, and to plan information security audits. Although the information asset register is managed by IT, consideration should also be given to the security of paper records.
2.6 Information assets are to be identified as logical collections. That is, information collected for a project could be held in various media including a number of laptops, a group space drive and USB sticks. This should be recorded as one entry describing each medium and how they are kept secure.

2.7 Departments must declare any information assets held by the department. Please list any additional systems purchased locally for digital/records storage, as 'departmental system' assets. Departments should contact IT Security via the IT Service Desk if they require advice in declaring additional information assets. Examples of such assets include cloud storage systems and paper filing systems.
2.8 When reviewing the information assets for their department, HODs should consider:
• Any new information assets that need to be added to the register;
• Any information assets that are no longer in use and can be removed from the register;
• Any information assets where use has changed, where the asset register needs to be updated;
• Any policy changes that affect the way information assets are used by the department.
2.9 It is recognised that HODs (or their delegate) will not have comprehensive knowledge of all the information which staff in their department are working with, or all the ways this information is stored. Departments are encouraged to reflect broadly on the key risks associated with information the department holds, and where this information is stored, when completing the information asset register. Departments may find it helpful to focus on the transmission of data, especially where data is sensitive or transmitted outside of the Company.

Appendix A: Structure of Information Asset Register – See Code of Practice Information Asset Register CoP D3.

Code of Practice 5
Electronic Messaging

Introduction
1.1 Electronic communication applications, including e-mail and calendar are important means of communication for the Company and they provide an efficient method of conducting much of the Company's business. This document sets out the Company's guidelines on the proper use of electronic communication applications for Company purposes, including teaching and administration. It describes the practices, rules and regulations, specifically in reference to security and data protection.
1.2 The Company use Office 365 service from Microsoft to provide an electronic communications platform which includes use of "Office" software by its staff and students. This guideline is intended to provide information about the use of electronic communications systems, including, but not limited to Outlook, Skype for Business, and Yammer.
1.3 A "message", as used in this document, is defined as any piece of written communication, attachment, recording, pITure, or any other file sent, received or published using electronic communications software.

2. Security
2.1 The contents of all email accounts may be accessed subject to approval through normal Company process with reasonable cause as explained in Section "Conditions of Use of IT Resources (Acceptable Use Policy)" in the Company's Information Security Policy.
2.2 Electronic mail and calendars are not secure services. For example, it is possible for unauthorised individuals to monitor the transmission of e-mails or calendar items, or to send counterfeit mail under a user's name. Therefore, users must not include any confidential or personal information in an electronic message unless the information is encrypted.
2.3 To enhance collaboration, calendar items including their subject lines may be available by

default for other Company staff to see. Therefore, staff and students must avoid putting any sensitive (including personal) information in the subject line of calendar items. The notes within a calendar item will not be visible to others by default including attachments. However, you should still avoid putting any sensitive or personal data in calendar items as per section 1. For a full list of sensitive data and protected personal characteristics see the Company's Information Security Policy and Data Protection Policy, respectively. Also note that, other personal information could be deemed as sensitive depending on the circumstances, e.g. names of people attending interviews, leave types of staff (such as appointments, domestic emergencies), etc. Subject lines of any private calendar entries could be made invisible to others by selecting the "padlock" icon to make them private.
2.4 Company e-mail accounts are accessible everywhere with the use of the "Outlook Web App" on any web browser software. When "Outlook Web App" is used, the session will time out after 1 hour when not active to avoid someone else gaining access to the account. After this duration, the system requires re-authentication by entering the user-name and password.
2.5 Please take care when addressing email communications and consider that the Autocomplete function may suggest a different email address to the one intended. If you send personal or sensitive personal data to an incorrect email address, please report this as a data breach using the published procedure.

3. Archiving, Retention and Deletion
3.1 All messages older than 2 years will be automatically moved to archive folders for new users. To search/find emails older than 2 years, users have to go to the "online archive" section. One of the following options can be selected to change this setting using the "Assign Policy" option under the "Home" menu:
• Do not archive (All e-mail messages will be kept in the default folders in Outlook (e.g. Inbox and Sent Items) and will not be archived automatically.)
• Archive e-mails older than 2 years.
3.2 E-mail messages will normally never be deleted. The following options are available to Company users to select from:
• Delete messages older than 5 years
• Delete messages older than 10 years
• Retain all messages indefinitely
3.3 If you select any of the "delete" options, your messages older than the specified number of years will be regularly purged without further notice.
3.4 When a staff member or student leaves the Company, their account will be soft-deleted, that is, disabled on the date of their departure. The email account will no longer be accessible. Six months after the departure date, the accounts will be fully deleted, which will trigger the complete purge of the mailbox after another 30 days. Staff members may request to retain their Company user-name/email account for continuity of Company business for up to six months. This must be authorised by their line manager and the Compliance Manager.
3.5 There is a Company policy and process that allows line managers to access staff members' emails and files for continuity of Company business after they have left. Staff members are encouraged to delete all personal emails and files before they leave.
3.6 When a student leaves, IT will offer them to get an Leaver email account on Google Mail. They will receive the information about the "Google email address for life" and they will be able to set this up if they prefer to do so.

4. Use of Non-Company Email and Forwarding
4.1 Company staff and students are provided with Company email addresses for email communication to be carried out in a safe and reliable way and give a level of assurance that emails have been delivered. This assurance cannot be provided in the case of Company staff and students using an external (non-Company) email accounts to carry out Company communications and auto-forwarding of emails to an external email account. Therefore, using an external email account to carry our Company business and auto-forwarding to external (non-Company) email accounts are not permitted.
4.2 If you believe you have a valid reason to redirect your Company email to an external email account, please raise a ticket with the IT Service Desk and this will be reviewed in line with the Company's Information Security Policy.
4.3 Emails of staff who have privileged access to one or more Company systems (e.g. System Administrators, DBAs) as well as staff with financial approval responsibilities must NOT be auto-forwarded under any circumstances.
4.4 For students, email auto-forwarding is only available after they have completed their studies and for the duration their Company email account is kept active.

5. Other
5.1 The Company provides access to e-mail systems for the conduct of the Company's business. Incidental and occasional personal use of e-mail is permitted within the Company so long as such use does not disrupt or distract you from conducting the Company's business (i.e. due to volume or frequency) or prevent others from accessing the network for legitimate Company business.
5.2 Trades Union representatives who are members of the Company may use the e-mail system to transact union business with their members.
5.3 All staff and students are encouraged to upload a recent photo of themselves as an icon photo to allow people to identify them on Microsoft Office 365 environment. However, if you prefer not to share your picture publicly, you should not use a picture other than a true reflection of yourself and should leave the icon picture as default.

Code of Practice 6
Passwords

1. Introduction
1.1 This Code of Practice defines the procedures and provides advice for managing and protecting passwords associated with all Information Systems at SB Skills Solutions.

2. Strong Passwords
2.1 The Company enforces the following criteria in order for users to select a strong password, and therefore achieve effective password protection:
2.1.1 A password must be at least 8 characters in length.
2.1.2 A password must contain at least three of the following four elements:
- Numeric Characters (0 - 9)

- Uppercase Characters (A-Z)
- Lowercase Characters (a - z)
- Special Characters (?, !, @, #, %, etc.)

2.1.3 A password should not contain any of the following:

- A word, either from a dITionary (any language), slang or common acronym.
- A name, of either a person or place.
- An easily guessable date, such as partner's birthday.
- Information related to you, such as your car number plate, NI number, CID number, etc.
- The same or close to your account username (including reversing or misspelling of the username)
- Any of the examples given on the IT website, or this Code of Practice.

2.1.4 The new password cannot be the same as one of the last 12 passwords used.

3. Password Protection

3.1 Users should choose a password that is memorable and avoid writing down passwords and under no circumstances leave a password in a place readily accessible to others.
3.2 Users should not disclose their password to others. IT will never ask for a user's password. The only person who needs to know your password is the user.
3.3 If a user becomes aware their password has been disclosed by accident or otherwise, they should change their password immediately and report it to IT.
3.4 A user should take care that it is difficult for others to see their password being typed in. Care should be taken as to who is watching.
3.5 Users should not enter their passwords into a website, unless they are sure that it is a legitimate Company system / website. The best method to ensure this is to access sites using your own bookmarks or typed-in URLs. Avoid using links especially from within emails claiming to be legitimate.

4. Changing Passwords

4.1 Company users are asked to change their passwords periodically. This is currently between 30 days and a year depending on roles and responsibilities of account holders.
4.2 You can change your password by logging on to a Company computer and using the link to reset-password
4.3 Recycling of old passwords is not allowed. This is a good practice you could also use for non-Company systems.
4.4 Users with passwords not in compliance with this Code of Practice will be required to change their password immediately.
4.5 Users who are required to change their password will be contacted via email, telephone or in person by a member of IT staff. Users should not reveal their passwords to anyone including IT Staff.

5. Passwords for External Systems

5.1 You are advised to follow the best practices provided in this Code of Practice when choosing passwords for non-Company systems.
5.2 You should not use your Company username and password for setting up accounts on websites or other Internet resources.

Code of Practice 7
Inspection of Electronic Communications and Data

1.Scope
The purpose of this Code of Practice is to prescribe the circumstances under which the Company may monitor of intercept electronic communications. It applies to staff, students and external third parties that have access to or permission to use the Company's electronic communications facilities.

2. Monitoring Electronic Communications
2.1 Electronic communications are broadly telephone calls, fax messages, all types of electronic messages including e-mails, instant messages, SMS or other short messages, tweets, published web contents including wikis, blogs, posts on messaging platforms, etc. The Company does not, as a matter of course, undertake general monitoring of the contents of staff or student electronic communications. Moreover, the Company does not routinely undertake random sampling or general scanning of electronic communications through human intervention. However automated computerised scanning of email traffic is performed for the purpose of intercepting unsolicited bulk email (commonly referred to as "spam") and potentially damaging message content (computer viruses, attempts at financial fraud etc.)
2.2 In accordance with the “Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000”, made under the “Regulation of Investigatory Powers Act 2000” (RIPA) 2000, the Company will exercise its right to intercept and monitor electronic communications received by and sent from the Company for the purposes permitted under those Regulations.
2.3 If an organisation intercepts a communication on its system without legal authority, the sender or the recipient of the communication will be able to obtain an injunction or, if they can show that they suffered a loss as a result of the interception, sue for damages. RIPA also establishes the circumstances in which it is lawful to intercept communications. It authorises interception in cases where the interceptor has reasonable grounds to believe that both the sender and intended recipient have consented. It also provides for the Secretary of State to make "Lawful Business Practice" Regulations setting out the circumstances in which organisations can lawfully intercept communications without consent.
2.4 Of relevance to the Company is the “Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000”. This allows organisations to intercept, without consent, for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use and ensuring the effective operation of their telecommunications systems. Organisations will not need to gain consent before intercepting for these purposes although they must have informed the users of the systems that interceptions may take place.
2.5 The purposes for which organisations will be able to intercept without consent under the Regulations are listed below. Depending on circumstances the Company may make use of some or all of these purposes:

2.5.1 Establishing the existence of facts relevant to the organisation, for example keeping records of transactions and other communications in cases where it is necessary or desirable to know the specific facts of the communication.
2.5.2 Ascertaining compliance with regulatory or self-regulatory practices or procedures relevant to the organisation, for example monitoring as a means to check that the organisation is complying with regulatory or self-regulatory rules or guidelines.
2.5.3 Ascertaining or demonstrating standards which are or ought to be achieved by persons using the system, for example monitoring for purposes of quality control or staff training.
2.5.4 Preventing or detecting crime for example, monitoring or recording to detect fraud, computer misuse or other illegal activities.
2.5.5 Investigating or detecting the unauthorised use of the systems, for example monitoring to ensure that employees do not breach Company rules e.g. “Conditions of Use of IT Resources (Acceptable Use Policy)” in Company’s Information Security Policy.
2.5.6 Ensuring the effective operation of the system, for example monitoring for and deleting viruses, checking for and stopping other threats to the system e.g. hacking or denial of service attacks, monitoring automated processes such as net flow logs, e-mails logs, caching activity and load distribution.
2.5.7 Determining whether or not the communications are relevant to the organisation, for example checking email accounts to access communication in staff absence.
2.5.8 In the case of communications to a confidential anonymous counselling or support help line, for example monitoring calls to confidential, welfare help lines in order to protect or support help line staff.
2.6 The Company intends to make interceptions for the purposes authorised under the Regulations and has made reasonable efforts to inform members of Company, who may use its system, that communications may be intercepted.
2.7 Users of Company communications should be aware that IT System and Network officers, from time to time, monitor transmissions or observe transactional information to ensure proper functioning of Company IT services. On these and other occasions such personnel might, inadvertently, become aware of the contents of electronic communications. Except as provided elsewhere in this Code of Practice or by law, personnel are not permitted to intentionally examine the contents of transactional information or disclose or otherwise use what they have seen, heard, or read. If, however, violations of Company policy or law are discovered they must be reported to Company authorities.
2.8 The contents of electronic communications and transactional records may be inspected to redirect or dispose of otherwise undeliverable electronic communications, e.g. that are addressed to Webmaster. Such unavoidable inspection of electronic communications is limited to the minimal level of examination required to route the otherwise undeliverable electronic communication to its intended recipients. Re-routed electronic communications must be accompanied by notification to the recipient that the electronic communication has been inspected for such purposes.

3. Inspection of Electronic Data
3.1 It may be necessary, from time to time, for the Company to investigate the data on networked or stand-alone Company owned storage, including but not limited to individuals’ Company emails, documents and files in local, home or group drives, account information, and logs, e.g. access logs to Company systems or premises. Furthermore, by connecting a privately owned device to the Company network, the user consents to allow the Company to inspect it in accordance with section 6 “Monitoring Electronic Communications” of Company’s

Information Security Policy. Any such inspection actions taken and any subsequent disclosures shall be in full compliance with the law, particularly the Data Protection Act 1998 and applicable Company policies.
3.2 Under normal circumstances, the user's consent will be sought by the Company prior to any inspection being carried out on data held by or related to individuals, e.g. Company email accounts, home or local drives, access logs, etc. However, in the following circumstances inspection will be carried out even though the user has not given consent:
3.2.1 when there is a legal requirement to do so;
3.2.2 when there are reasons to believe that violations of law or of Company policies may have taken place, e.g. where there is reliable evidence as distinguished from rumour or gossip;
3.2.3 when there are compelling/emergency circumstances, for example when failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of Company policies, or significant liability to the Company or to members of the Company community;
3.2.4 when failure to act could seriously hamper the ability of the Company to function administratively or to meet its teaching/research and related obligations.
3.3 If inspection of data held by or related to individuals is required for business reasons while the account holder is away from the Company, the consent of the account holder must first be sought. If the account holder cannot be contacted, the Head of Department and the SIRO must jointly authorise the inspection in writing. Both a record of the measures taken to obtain consent, and the basis for allowing the inspection must be recorded.
3.4 In instances where data held by or related to individuals are to be lawfully inspected due to circumstances listed in section 3.2.
3.4.1 Emergency Circumstances: The minimal perusal of contents and the minimal action necessary to resolve the emergency may be taken immediately without authorisation, but appropriate authorisation must then be sought without delay and recorded;
3.4.2 All other circumstances: Inspection must be subject to the prior joint authorisation, in writing, by the Head of Department and the SIRO/DPO.
3.4.3 Encrypted Information. When a system is found to contain encrypted information, a relevant decryption key must be provided upon request.
3.4.4 Data created by or related to staff/students no longer employed by or studying at the Company left on Company systems is the property of the Company. It is not necessary to seek the permission of the former member of staff/student before such information can be inspected. Authorisation to view information must be sought jointly from the Head of Department and the SIRO/DPO.
3.5 Once authorisation has been granted, any information found on a system shall be treated in the following manner:
3.5.1 Company/Work related material shall be dealt with in line with normal working practices and retained or deleted, as necessary.
3.5.2 Material that appears to be of a personal nature will only be inspected if there is a legitimate business reason for doing so.
3.5.3 Members of Company are responsible for removing any personal information from their electronic documents and emails before their departure.
3.6 Privacy. Any inspection, authorized under this CoP, shall be conducted with due regard to the right to privacy. Material that appears to be private shall be subject to the minimal inspection required to conclude the search. Any confidential information encountered which is not related to the purpose for which the search was undertaken shall not be disclosed to any party and shall remain confidential. However, if material is accidentally discovered in the course

of an inspection which is either illegal or contravenes Company policies, the matter will be referred to the SIRO/DPO, who may authorise further investigation.

Code of Practice 8
Clear Desk and Clear Screen Policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted for all staff as follows:

Clear Desk
SB Sills Solutions is committed to maintaining a professional and presentable working environment and to ensure that high standards of data security are demonstrated effectively. This policy along with our Data Protection, Information Security and related Codes of Practice set out our required standards of information handling and processing.

Aim
The aim of the policy is to:

- Preserve a professional, presentable working environment
- Protect sensitive documentation and confidential information
- Increase productivity
- Help to reduce stress
- Reduce the amount of paper used
- Increase efficiency and flexibility by enabling the use of host desks.

Scope
This policy applies to all employees and other people who work for us.

Responsibility
It is your responsibility to familiarise yourself with and adhere to the guidelines set out in this policy, especially during periods when your desk is not within your direct line of supervision.

1. Secure and lock away all sensitive documents and information when you are not attending them.
2. Lock your computer to password protect it when not being used.
3. Ensure that paperwork containing customer personal data is never left unattended
    a. Ensure printing is collected immediately and is safely delivered to its intended destination.
    b. Place documents on your desk face down where there is a risk that a customer may see other's information.
    c. Check the paperwork you are handing out to customers to ensure it is 100% their own paperwork.

At the end of the working day, your desk should be cleared of all sensitive documents. You should put sensitive documents or confidential information in a secure locked place. We do not consider desks and pedestals secure for overnight storage. Please use the Administration filing cabinets for this purpose and they should be kept locked when not in use and at the end of each day.

When documents are no longer needed you should ensure that, if they contain sensitive information, they are placed in the confidential waste containers or shredded depending on the facilities available at your site. The normal waste bins are NOT secure disposal routes.

Actions
In order to keep your desk clear you should: (Please refer to Information Security Policy)

1. Allocate time in your calendar to clear your paperwork;
2. Always clear your workspace before leaving it for longer periods of time;
3. Use the secure confidential bins for sensitive documents when they are no longer needed;
4. Lock your desk and any filing cabinets at the end of the day; and
5. Treat mass storage devices such as CD-ROMs, DVDs or USB drives as sensitive documents and secure them in a locked drawer when not in use.

Monitoring
We will monitor this policy on an ongoing basis. If you are found to be in breach of this policy, you may be subject to disciplinary action in accordance with our Disciplinary Policy.

Clear Screen
If you leave your workstation unattended, you must either lock the system or close it down and log off.

Code of Practice 9
Archiving

Introduction
Background

- SB Skills Solutions holds a growing number of contracts which require ongoing archiving. Archives range from Training to Welfare to Work and all are housed within the Archive Store Facility. Work began to establish the Company's archives during 2018 and is available for all contracts.
- SB Skills Solutions has an obligation to implement and preserve good archiving procedures and processes.

The secure Archive Store Facility is housed in the SB Skills Solutions HQ Admin. Centre.

Definition of Terms
The following terms are used in this policy:
Archival Value
Also called historical value, continuing value, enduring value and permanent value. In general, the value of records for future use as evidence of past activities.
Archives
Original records which have been selected for semi-permanent preservation because of their continuing value, especially those materials maintained using controls governed by relevant funding organisations.

Claims Department
The Claims team are responsible for acquiring, arranging, preserving and providing access to records of enduring value held by SB Skills Solutions.
De-accessioning/disposal
The process by which the permanent removal of materials from archive is executed, either by transferring them to another company (contract withdrawal) or destroying them through secure shredding once destruction dates are met.
Depositor
A person that transfers custody of historical records to SB Skills Solution's Archives.
Records
Recorded information that has been fixed in any form, which has content, context and structure, created or received by a person or organisation in the transaction of business or the conduct of affairs.

Definition of Archive
Some common definitions of archives are:

- Records that are preserved permanently because of their enduring value.
- The building, room or storage area where archival files are kept.
- An organisation responsible for arrival material.

SB Skills Solutions extend this to include records that are preserved semi-permanently and those records, which are stored where it is not feasible to include them in situ in the office environment.

Archival Records

- SB Sills Solutions archival records are those records which are no longer current but which have been chosen to be preserved, for a specific length of time due to contract requirements.
- The records that are eligible to become archives may need to be kept permanently because they are evidential, or for some other legal reason. They may have a business need value.
- These records may be original documents, often unique, and they may be irreplaceable. An archival record may be the only copy that exists anywhere.
- Archival records could be in any format or medium. They can exist electronically, although the vast majority will be paper.

Aims & Objectives
The aims of SB Skills Solutions are:

- To Collect and Preserve records of financial and other importance, through the effective use of contract compliance and secure management of the Archive Store.

The objectives of SB Skills Solutions are:

- To acquire, preserve, catalogue and make available files of continuing evidential value
- To preserve new and existing records for current and future use
- To adhere to Data Protection security at all times

Collection policy
SB Skills Solutions collects and holds all archive files to support contract compliance. Records can be internally transferred using a sign out system that is currently in place and controlled by the Claims team.

De-Accessioning
The purpose of SB Skills is to retain records of value in relation to contracts that have/are being delivered. A periodic review of the records held, in line with contractual requirements shall be carried out. Records held which fall outside this policy should be removed from the archives and securely destroyed. Only files that clearly fall outside of these conditions may be de-accessioned. Only files chosen for de-accessioning shall be destroyed.

Exceptions
Exceptions may be made to this policy in instances where SB Skills Solutions or subsidiary is a Sub Contractor to a Prime Contractor. In such cases, the Prime may enforce their own Archiving policy which will be executed by the claims team after being assessed for Risk to SB Skills Solutions by the SIRO/DPO.

Code of Practice 10
Document & Media classification Policy

Introduction
Data classification can be loosely defined as organizing data into categories based on the content so that access rights can be appropriately assigned, and security can be focussed. Data classification makes data easier to locate and retrieve. This can be useful in cases where subjects exercise their right to be forgotten, for example. Data classification involves tagging data so that it can be easily searched for and monitored.

The Benefits of Data Classification
In general terms, there are three key benefits to perfecting your data classification strategy:
Meeting Compliance Demands: One of the most popular reasons why organizations look to implement data classification, is to help ensure they can meet regulatory compliance requirements. Most compliance requirements mandate that data is searchable and retrievable within very tight deadlines.
Improving Data Security: Data classification is also useful when it comes to protecting your sensitive data. The first step in a data-centric approach to security is to ensure you know where your most sensitive data is located and the reason why it is deemed to be sensitive. Once you know this, you will be in a better place to decide what access rights to apply on the data, which users actually need access, and be able to focus your user behaviour analytics on the data and users that matter most.
Understanding a Breach: Should the worst happen, and you suffer a data breach, data classification will help you to determine the extent of the damage, what data was lost and help guide who to inform.

Classification Levels
There are commonly shown to be four classification levels that you can adhere to when it comes to classifying your data – and they are presented in order of most to least risk.

Restricted: this data poses the biggest risk to your organization and must be kept secure. Loss or theft of this data could cause significant harm to your business and to the individuals affected and incur criminal or legal liability.
High Risk: This is data that, if exposed, could cause harm to the business and the individuals affected, including the potential for legal action. It is data usually covered under compliance regulations, including protected health information and personally identifiable information.
Medium Risk: If this data is exposed it could cause limited harm to individuals and to the business, such as business contracts with third-parties, intellectual property and employee records.
Low Risk: Public information that would not cause any harm to individuals or the business if exposed. Such data includes anything that is in the public sphere, such as published Data.

Personal Data
Standard Personal Data - this is defined in Article 4 of the General Data Protection Regulation as any information relating to an identified or identifiable natural person (referred to as a 'data subject'), where 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. The collection, use and retention of personal data must comply with strict conditions and such data requires special measures of protection as more particularly described in SB Skills Solutions Data Protection Policy;
Sensitive Personal Data (also known as special categories of data) is a subset of personal data - this is defined in Article 8 of the General Data Protection Regulation as 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. The processing of sensitive personal data is subject to additional requirements and requires additional protections also as described in more detail in our Data Protection Policy;
N**on-personal Data** (organisational data) which can be:
a. sensitive organisational data which includes commercially sensitive, data protected by confidentiality agreements, legally privileged information, etc. This data should be protected by appropriate protection measures; and
b. non-sensitive organisational data which is data pertaining to SB Skills Solutions not published by default, but which may be disclosed (subject to legal advice) in response to requests made under the Freedom of Information Act.

The ‘need to know’ Principle
The effective use (including the sharing and protection) of information is a key priority for SB Skills Solutions. Access to sensitive information or assets will only be granted to those who have a business need and the appropriate personnel security control (PSS). This ‘need to know’ principle is fundamental to the security of all protectively marked information and assets. If there is any doubt about giving access to sensitive information or assets staff should consult their HOD managers before doing so.

Applying Correct Protective Marking
The originator or nominated owner of information, or an asset, is responsible for applying the correct protective marking. If applied correctly, the Protective Marking System will ensure that only genuinely sensitive material is safeguarded.

- SB Skills Solutions documents that are not public shall be classified in one of the following categories: confidential or restricted. Criteria and guidance for classification are set out in Annex 1 to this decision.
- Applications for access to classified documents shall be examined by Head of Department or member of the SMT.
- If a classified document is to be made available in response to a request from a member of the public, it shall be first declassified by a decision of the SIRO/DPO.
- Documents shall be classified only when necessary. The classification shall be clearly indicated and shall be maintained only as long as the document requires protection/destruction.
- The level of its contents, value, legal requirements, sensitivity and criticality to the organisation shall determine the classification of a document.

Annex 1 - Criteria and Guidance for Classification of Documents

Classified Documents
Access to classified documents by members of the public is subject to examination of the SIRO/DPO.

Criteria for assessing CONFIDENTIAL assets:
Documents are confidential when their unauthorised disclosure could harm the essential interests of the individual, SB Skills Solutions, its clients or 3rd parties.
Commonly accepted criteria for confidentiality are where the release of a document would:

- Harm the privacy and integrity of an individual, staff member or customer;
- Breach the undertakings to respect the confidential nature of information provided by third parties;
- Breach statutory restrictions on disclosure of information;
- Cause financial loss or facilitate improper gain or advantage for individuals or companies;
- Impede or undermine the effective management or operations of SB Skills Solutions;

Documents classified as confidential include:

- Personnel files of SB Skills Solutions staff containing details of recruitment, promotion and medicals;
- Documents containing financial and commercial information supplied by third parties;
- Customer/client/staff files containing personal details including date of birth, national insurance number, address etc.

Criteria for assessing RESTRICTED assets:
Documents are restricted when their unauthorised disclosure would be disadvantageous to SB Skills Solutions, its clients or a third party. Documents with this classification are usually restricted for a period of time.
SB Skills Solutions documents falling under this category may include:

- Documents of internal management meetings;
- Documents of groups involved in the preparation of bids/ITT's etc;
- Documents that have not been finalised;
- Documents containing sensitive details supplied by customers, staff or third parties in confidence.

Criteria for assessing PROTECT (Sub-national security marking) assets:

- cause distress to individuals, customers, and members of staff;
- breach proper undertakings to maintain the confidence of information, provided by third parties;
- breach statutory restrictions on the disclosure of information;
- cause financial loss or loss of earning potential, or to facilitate improper gain;
- unfair advantage for individuals or companies;

Downgrading Classified Documents

Classification of documents shall be periodically reviewed. By request of the SIRO/DPO, the originator of a document shall indicate if that document or information may be downgraded and declassified. Where a document or information is declassified, details shall be recorded in the register and the document shall be archived appropriately. Where classification is retained, details of the review shall be entered in the register.

Physical Security

All classified documents shall be retained in a manner that ensures they are not disclosed to unauthorised individuals. Only the SIRO/DPO or a delegate member of SMT/Head of Department shall record classified documents in accordance with the Asset Register control Policy .

Only the Claims Team may retain classified documents in relation to our customers to ensure they are physically safeguarded.

Annex 2 - Classification Procedures

- Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classifications and shall be classified accordingly. The classification of a document as a whole shall be that of its most highly classified part.
- The originator shall indicate clearly at which level a document should be classified when detached from its enclosures.
- The classification shall appear at the top and bottom centre of each page, and each page shall be numbered. Each classified document shall bear a reference number and a date.
- All annexes and enclosures shall be listed on the first page of a document classified as confidential
- The classification shall be shown on restricted documents by electronic means.

It is the responsibility of the document owner to determine the classification of their document in line with this policy and SB Skills Solutions has decided that the following classifications are to be used;

1. Confidential
2. Restricted
3. Protect
4. Unclassified

Code of Practice 11
File Control Policy

Introduction
Background

- SB Skills Solutions holds a growing number of contracts which require ongoing access to Customer Files, contracts range from Training to Welfare to Work and all live files are housed within locked cabinets in secure areas.
- SB Skills Solutions has an obligation to implement and preserve good File control procedures and processes.

Policy Statement
The aims of SB Skills Solutions are:

- To ensure all client files remain confidential with only authorised personnel having access.
- To implement and maintain secure use of all client files
- To adhere to Data Protection security at all times

Collection Policy
SB Skills Solutions collects and holds all live client files to support contract compliance. Records can be internally transferred using the sign out system that is currently in place. This is held and managed by contract management and audited on a weekly basis by the relevant Head of Department or a member of the SMT .
As an example of the information required the collection record we need:

- File details;
- Current owner and permission status;
- Sign-out signature, date and time;
- Return date, signature, date and time;

Code of Practice 12
Shredding & Disposal Policy

Introduction
All organisations deal with information and this must be managed correctly and effectively. As such, it is important that all formats of the information are addressed. This policy addresses paper information and provides three main benefits to an organisation:

- Gives guidance and legitimacy to shredding and disposal of paper documents
- Ensures consistency of practice within SB Skills Solutions
- Helps ensure that paper information is kept for the correct period of time.

Purpose of Policy
SB Skills Solutions hold a number of contracts, whose client files must be retained for a set period of time, once these contracts end, this policy establishes a framework for the destruction of paper documents. The means of destruction will be shredding, whether this is in house or by

the use of an external confidential waste management company. At the time of reviewing this document it has been decided to keep shredding in-house.

Rationale for Policy
SB Skills Solutions need to ensure all appropriate staff understand the rationale and goals for this policy:

- To ensure correct destruction of information and adhering to the correct timeframe
- To reduce space and storage costs (where applicable)

Scope
This policy covers all paper documents at all classified security levels.
This policy applies to all staff regardless of role within SB Skills Solutions.

Policy
There are three main classifications of paper documents:

- A-type – non-business documents – junk mail, flyers, leaflets etc.
- B-type – Business documents – able to have authorised copy (e.g. scanned, email, fax)
- C-type – Business documents – must have original document (e.g. client file, job stencil)

All paper documents created or acquired by SB Skills Solutions will fall into one of these classifications. If you require clarity, please discuss individual cases with the administration team or DPO.

A-type Documents
A-type documents have no lasting business value and do not require any period of retention and these documents can use any type of classification of shredder.

B-type Documents
B-type documents can be destroyed under two different situations:

- When an authorised copy has been made in which case the authorised copy is then held under the retention period.
- Destroyed in line with the retention period being achieved.

B-type documents must be shredded using a cross-cut shredder and the shredded paper disposed of securely, this must be done in accordance with the HMG requirements (Shredder must produce a shred size of 4mm x 15mm). The shredder currently used in house exceeds the HMG requirements.

C-type Documents
C-type documents can only be destroyed according to the retention schedule in accordance with the Contract Funding Body requirements. All copies must be destroyed at the same time using a cross-cut shredder and in accordance with the HMG requirements (Shredder must produce a shred size of 4mm x 15mm). The shredder currently used exceeds the HMG requirements.

Roles and Responsibilities
In order for this policy to work and be effective, roles and responsibilities must be assigned:

Responsibility for the policy – SIRO/DPO or his delegate.
Authorise Destruction – Administration Team Manager after consultation with SIRO/DPO in line with contract funding organisation
Destruction of the paper documents – Administration Team Manager will delegate or oversee a member of their team
Record of disposed documents – This will be recorded on the archive list and will be completed by the Administration Team Manager or an appropriate designated member of that team.

Retention Schedules
This policy does not cover retention schedules as SB Skills Solutions hold many contracts with many different retention dates; it simply supports the destruction of paper documents in line with Contract Funding body guidelines.

Code of Practice 13
Equipment Policy

Introduction
This document aims to provide a framework for the acquisition, deployment, maintenance, audit, loan, hire, renewal and disposal of items of equipment that are on the companies equipment register.

Scope, Deployment and Definition of Equipment
Equipment purchased using SB Solutions (the company) funds should be for the companies use and should be regarded as a company resource. In many cases equipment will be used mainly by one department area and will be prioritised to that area. However, equipment should not be considered as being owned exclusively by a departmental area; this should allow equipment to be shared wherever practicable. It follows from this that an up-to-date equipment register must be maintained so staff are aware of all the equipment available within the company.
For the purposes of this policy, equipment will be defined as items which:

- cost over £50
- are on the company equipment register

Exceptions include

- Furniture such as tables, desks, chairs, drawers, filing cabinets, cupboards, notice boards, blinds, plumbed in fixtures, towels and curtains.
- Minor equipment costing less than £50, which would be the responsibility of the appropriate head of department where it is used.

Equipment will be either prioritised to a specified department (Prioritised equipment) or will be for more general use across the company (General equipment).
Heads of Departments and the staff in training areas will be responsible for the siting, care, secure storage and upkeep of all prioritised equipment in those areas.
'General' equipment will be assigned to a specified individual and the siting, care, secure storage and upkeep of this equipment will be that individual's responsibility.

Decision-Making
All decisions about the purchase of new equipment and the repair/ replacement of broken / defunct equipment will be made by the Senior Management Team (SMT).

Acquisition of New Equipment
Staff will be able to make written proposals to the Senior management team for the acquisition of new equipment at any time, though most requests will be expected in accordance with the budget setting timetable.

Safety
Staff using equipment have a responsibility to ensure they are aware of any Health and Safety implications and are responsible for ensuring students are aware of appropriate safety procedures.

Risk assessment should be made for all items of equipment in accordance with the Health and Safety policy. Individuals responsible for equipment are also responsible for maintaining records of these assessments.
Training in the use of equipment and undertaking risk assessment should be sought where necessary.
All electrical equipment should be checked annually for electrical safety. Records of this check will be kept by the Health and Safety Officer.

Security
All items on the equipment register will be allocated a number. Where practicable, this will be clearly marked on the item itself.
If an item of equipment goes missing by theft or other means, this should be reported via our security incident process, (Appendix 1).
All new IT equipment should be passed to the Head of IT/Compliance Manager *or* delegate prior to it being issued for use, so it can be marked and entered on the equipment register.

Audit/ Record-Keeping
Details of all items of equipment as defined in this policy should be kept on the company equipment register.
An annual audit to check and update the equipment register should be co-ordinated by the Head of IT/Compliance Manager /Compliance Manager.
The equipment register will:

- Be held on an electronic data base
- Include extended guarantee details.

The Head of IT/Compliance Manager /Compliance manager or a delegated representative will be responsible for keeping the equipment register up-to-date.

Maintenance
Where appropriate and affordable, maintenance contracts should be taken out for expensive and crucial items of equipment (e.g. photocopiers and file servers). Decisions regarding which items to cover by outside contracts should be made by the Head of IT/Compliance Manager /Compliance Manager and Senior Management Team.
Individual staff using equipment should pass on minor repair needs to the IT support or to the Head of IT/Compliance Manager .

Disposal
Any item no longer in use should be notified to the Head of IT/Compliance Manager. The Head of IT/Compliance Manager will consider the most appropriate and economic method of disposal. Consideration will be given to age, condition, residual value, further use in the Company. The method of disposal will then be determined. The equipment register will be updated by Head of IT/Compliance Manager detailing date and method of disposal.

Loan and Hire
The IT team will decide which equipment is available for loan and/or hire. The IT team will delegate to specified individuals the responsibility for recording (in duplicate) the loan/hire and return of equipment. A standard procedure, determined by the equipment team, should be used for recording the loan and return of equipment. This will include

- Standard paperwork recording details of the loan and the expected return.
- Guidance on the safe use and security of equipment.
- Information about whose is the responsibility for the equipment loaned.

Code of Practice 14
Audit Policy

Aims
Auditing aims to provide evidence for confidence that an organisation can "operate in a controlled and consistent manner, in the ways it has defined, subject to external requirements". Thus SB Skills Solutions (the company) must respond to the requirement of its customers/clients while satisfying the needs of awarding bodies and data regulation compliance. If the full benefits of an audit are to be realised, it must never be seen as an opportunity for conflict, retribution or punishment. Audit is not about blame nor is it concerned with the personal appraisal of the individual in his/her work role.

Audit Process
An audit is a systematic examination to determine whether or not activities and their associated results comply with planned arrangements and stated standards. It will also seek to determine if arrangements are implemented effectively and whether or not they are suitable to achieve the stated objective. The Administration team will carry out Audit checks prior to claims being submitted. A sample of work along with independent checks will be carried out by the Quality Assurance Team alongside the SIRO/DPO and COM.
While a degree of independence is required in the Administration Team, there is also benefit derived from including representation from the area to be audited. The company approach will be to partner, when appropriate, core audit staff with representatives from the area or aspect to be audited. We also ensure that Administration and Claims team staff are not line managed by Operations HOD Managers or SIRO/DPO.
Those with a major involvement will be the Quality Assurance Manager/Team and the Administration/Claims team alongside the SIRO/DPO.

Claims Audit Activity
The thrust of the audit activity will be:

- To identify areas where internal and external requirements are not being met. This will allow assistance to be provided to achieve stated standards and implement required standards effectively in respect of recorded objectives.
- To identify any data security or protection issues alongside IT log audits.
- To aid identification of areas of good practice and facilitate dissemination of these across all contracts held by SB Skills Solutions.
- Frequency of audit activity for subcontracts will be determined by the Prime Contractor; and may be carried out by a member of the operations team on condition that sufficient independent checks are carried out by the Prime Contractor.
- Frequency of audit for Prime contract activity is to be determined in conjunction with the contract holder. Changes to funding scenarios will trigger a 100% check in the next claim by independent audit, reducing to 50%, 20%, 10% in subsequent claims if sufficient data integrity is demonstrated.

Internal Data Protection and Security Audit

Internal auditing is based on the following pre-conditions:

- Existence of identified and recorded external requirements.
- The management systems are formally written down in terms of defining tasks and identifying records.
- Once variances are identified any reasonable steps are taken to eliminate them by the appropriate Heads of Departments/SMT.
- The lead auditor is independent of the area of the audit.
- The Audit Process works in harness with the development of a quality culture. Emphasis will be placed on self-evaluative reviews, supported centrally.

Audit Calendar

Audits will aim to be conducted with the minimum disruption to normal working patterns and be limited to the period of time allocated.
Prime contracts will be inspected on a monthly basis on the final week of the period before claims are made under the following schedule:
7 days prior to claim deadline: All claims are identified from subcontractors.
3 days prior to claim deadline: All audits are complete to verify the claim.

Audit Exemptions

In situations where regular, funder initiated or recognised external audit takes place, the results and feedback may be used in proxy of our internal audit verification.

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 Manager - 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

Next Review January 2022