SB Skills Solutions
Information & Data Governance Framework (IDGF)

This Policy should be read in conjunction with all Data Management and Information Governance Policies and related Codes of Practice (CoPs) including:

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

SB Skills Solutions
Information & Data Governance Framework (IDGF)

1. Introduction

1.1 This document constitutes the SB Skills Solutions Information Governance Policy Framework. It gives an overview of the policies, codes of practice, and guidelines that apply to information and data governance and security and sets out our commitment to providing training and increasing awareness in this area.

1.2 This Framework pulls together all the requirements for information governance so that all information is processed legally, securely, efficiently and effectively. Information plays a key part in our day to day operations and governance. The quality of our services, planning, performance measurement, assurance and financial management relies upon accurate and available information. Robust information governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. Accordingly, this Framework sets out the requirements, standards and best practice that apply to the handling of information.

1.3 Information governance is a key responsibility of each and every member of our community. Everyone has a part to play in implementing and embedding our policies and codes of conduct into working practices. Staff and students must familiarise themselves with this Framework and the policies it describes. This Framework and the information governance guidelines and regulations it contains are also expected of any third parties handling information.

1.4 The aim of this Framework is to help SB Skills Solutions:

- comply with its legal, regulatory and contractual obligations;
- maintain robust corporate governance;
- deliver high quality services;
- deliver value for money and protect the public funds entrusted to it;
- put in place appropriate business continuity arrangements;
- continuously improve the way we handle, utilise and protect information.

1.5 SB Skills Solutions holds and processes huge volumes of standard and sensitive data (as defined in Section 2.3 below) that is necessary for service provision, commercial engagement, and the safeguarding of everyone across the company estate.

2. Scope

2.1 This Framework covers all information held by SB Skills Solutions whether in electronic or physical format including by way of example:

- electronic data stored on and processed by fixed and portable computers and storage devices;
- data transmitted on networks;
- information sent by fax or similar transfer methods;
- all paper records;
- visual and photographic materials, slides and CCTV Information;
- spoken, including face-to-face, voicemail and recorded conversation.

2.2 The following are expected to comply with the Framework:

- all staff, and students;
- any third parties handling, or having access to, our information including for example consultants, service providers and contractors, visitors, volunteers.

2.3 The Framework is split into two parts – the first part describes our overarching information governance strategy and the second part sets out the information governance roles and responsibilities, policies and training.
2.4 The following is the classification template in accordance with which most of our data can be classified:
(1) **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;
(2) **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;
(3) **non-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.

3. Information Governance Strategy

3.1 Purpose of the strategy

3.1.1 The aim of this strategy is to enable SB Skills Solutions to meet its information management and security responsibilities so that customers, businesses, partners and suppliers have the confidence that information is handled and stored with due regard to its value and risk. Individuals must understand the importance of using information correctly, of sharing it lawfully and of protecting it from improper use.
3.1.2 The intention of this strategy is also to enable SB Skills Solutions to meet its legal and ethical obligations in terms of:

- the use and security of personal identifiable information;
- appropriate disclosure of information when required;
- regulatory frameworks for the management of information;
- professional codes of conduct for consent to the recording, sharing and uses of information;
- operating procedures and codes of practice adopted by SB Skills Solutions;
- information exchanged with third parties.

3.1.3 The strategy recognises the high standards expected of SB Skills Solutions as well as the ongoing task of maintaining appropriate standards of security in the area of information governance and of embedding a security culture fully throughout the organisation.

3.2 Strategic Objectives

These are the overarching information governance objectives of SB Skills Solutions. We want:

- information governance at SB Skills Solutions to be an enabler to overall strategy as well as to the underlying departmental strategies and business transformation programmes and for information assurance practices to be embedded within the design and implementation of such strategies and programmes;
- the infrastructure and processes for service delivery to provide the right information to the right people at the right time for the right purpose and promote the provision of high quality services by promoting the ethical, legal, effective and appropriate use of information;
- to provide innovative solutions to information governance issues with a view to transforming business processes;
- to promote information governance ensuring that it is embedded throughout the organisation and to direct organisational wide cultural change so that information is regarded as a key asset;
- to build into staff competencies and job descriptions specific requirements around the governance of information;
- to encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- to work to achieve required standards to comply with legislative, regulatory and contractual obligations and relevant policies;
- to identify and support effective practice in the management of information across all business areas, including preventing duplication of effort and enabling efficient use of resources;
- to identify and manage information assets across SB Skills Solutions and introduce an information risk management regime that balances risks with opportunities;
- to implement and operate proportionate controls that apply best practice standards to protect information assets and give confidence to all interested parties;
- to provide adequate training to all staff and key partners, increase awareness and embed a culture of care and responsibility in the handling of all information throughout the Company.

3.3 Approach

3.3.1 Information governance and assurance are integrated into all aspects of SB Skills Solutions operations. In delivering information governance services, four key elements of SB Skills Solutions operations will be considered:

- people
- process
- information
- technology

3.3.2 All information governance, improvement and assurance activities will consider how these factors need to operate in combination to achieve our strategic objectives.

3.3.3 The delivery of our information governance strategic objectives will be through a range of projects and a dedicated Information Governance Improvement Programme. The Improvement

Programme will define each information governance project, and these will be implemented and monitored in accordance with the stated governance arrangements and the approach detailed within this Framework.

3.4 Benefits

The following benefits (which are not an exhaustive list) provide an overview of the main benefits that should be derived through the delivery of this strategy:

- consistent and effective management of information across SB Skills Solutions;
- increased understanding of and compliance with relevant legislation;
- reduced number of information security incidents;
- reduced staff time and effort;
- improved data quality;
- clear responsibilities in relation to Information Governance and Assurance;
- effective management of information risks;
- greater confidence that information risks are effectively managed;
- better management of research data, with protection of intellectual property.

3.5 Strategy Governance

The Framework policies/codes of conduct and overall strategy governance is overseen by the Board of Directors and implemented and developed by the designated Senior Information Risk Owner and Data Protection Officer (SIRO/DPO) supported by the compliance Manager, Senior Management Team and Heads of Departments. See section 4 below.

4. Key Roles and Responsibilities for Information Governance

4.1 Board of Directors

Overarching information security and data protection governance (IG) resides with the Board of Directors with IG reports a standing item on monthly board meeting agenda. The Board appoints a board member as joint Senior Information Risk Owner and Data Protection Officer with responsibility for IG who reports to the Board on a monthly basis on all aspects of IG and the Framework. The Board agrees the IG strategy and improvement programme for the coming year, based on agreed priorities and available resources, and SIRO/DPO is responsible for monitoring and reporting progress on IG and improvement programme throughout the year. The information governance strategy will be implemented through the agreed policies, training, improvement programmes and through wider agreed change projects as agreed by the Board.

4.2 Senior Information Risk Owner and Data Protection Officer (SIRO/DPO)

SB Skills Solutions SIRO/DPO is the Accountable Officer who has overall responsibility for ensuring that information risks are assessed and mitigated and who has overall responsibility for disseminating policy, training and awareness to all who need to know within SB Skills Solutions. Information risks are handled in a similar manner to other risks, such as financial, legal and reputational risks. The DPO is the focal point for all activity within SB Skills Solutions relating to data protection. See SB Skills Solutions Data Protection Policy for details.

4.3 IT/Compliance Manager (CIM)

The SIRO/DPO is directly supported in both roles by the Compliance/IT Manager with more general back-up from the Senior Management Team and is accountable for ensuring this policy framework and attendant policies/codes of conduct are compliant, fit-for-purpose, implemented across the organisation with regular training, and continually up-dated and improved.

The Senior Information Risk Owner (SIRO) & Data Protection Officer (DPO) is Neil Beaumont, Director & Operations Director, supported by the Compliance & IT Manager (CIM) is Steve Maddocks.

4.4 The Senior Management Team (SMT)

The SMT facilitate the dissemination of data protection communications and maintain the enterprise vision, strategy and programme to protect information assets and systems across departments and divisions.

4.3 Heads of Departments (HODs)

HODs are responsible for consideration of Information Governance implications across their department and when working with partners. See the Information Security Policy for specific responsibilities relating to information security. HODs also act as data protection co-ordinators and information asset owners in their relevant department or division dealing with more routine data protection queries and guidance and assigned owners of information assets as listed in Information Asset Register-D3 and for assessing information security and data privacy risks annually applying the Data Privacy Impact Assessment Code of Practice -D4.

4.4 IG Continuity Steering Group & Incident Response Team (CIRT)

In the event of any potential threat or need for regular on-going support, cover or back-up the SIRO/DPO also assigns a small steering group and incident response team of SMT managers/directors (Paul Beaumont, John Kilner, Helen Best) to work alongside and in support of the IT Response Team.

4.5 IT Response Team and Service Desk (RST)

The IT response team and service desk support the CIM and manage day-to-day IG needs and services for staff and students.

These teams, the CIM, the SMT and HODs all report to the SIRO/DPO and act as forums to provide advice and propose changes to policies and codes of practice, particularly on changes to information security and on reports of information security incidents, as well as on remedial actions.

4.6 Staff, Students and Authorised Third Parties

All SB Skills Solutions staff, students and academics as well as authorised third parties who use and have access to SB Skills Solutions information must understand their personal responsibilities for information governance and comply with the law. All staff must comply with SB Skills Solutions policies, procedures and guidance and attend relevant education and training events in relation to information governance.

5. Framework Policies, Privacy Notices and Codes of Conduct

The **Information & Data Governance Framework (IDGF)** should be read in conjunction with other Data Management and Information Governance Policies and related Codes of Practice (CoPs) including:

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

6. Review, Induction and Training

New users of IT facilities, staff, students and approved third parties, should be instructed on the Company policies and Codes of Practice relating to information security and data protection. They should also be given training on the procedures relating to the security requirements of the particular work they are to undertake and on the correct use of the Company's IT assets in general before access to IT services is granted. It is the responsibility of managers that their staff are suitably trained, and to maintain training records.

8.2 All new staff of the Company are expected to complete the Company's online security awareness training and a data protection e-learning course (these are currently included within SB Skills Solutions induction and on-going refresher training mandatory for all Company staff. Staff must also attend the IT security inductions when joining the Company and must be aware of the latest IT security advice.

The policy documents, CoPs, and PNs comprising this IG Framework encompass all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read these document in their entirety and sign the form confirming they have read and understand policies fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into policies and distribute it all employees and contracts as applicable. Violation of the standards, policies and procedures presented in these documents by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

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

- As well as Privacy Notice awareness training for students information governance and data protection policies are actively promoted and highlighted across the delivery spectrum and embedded in all service transactions.

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

Version History Version/Status

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

Next Review January 2022