NHS
Bath and North East Somerset,
Swindon and Wiltshire
Integrated Care Board

BSW ICB Information Governance Framework

BSW ICB policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Policy Title

Purpose	Framework for BSW ICB information governance activities, management and governance
Document type	Policy
Reference Number	IGP01
Version	4
Name of Approving Body	BSW ICB Board
Operational Date	16 March 2023
Document Review Date	June 2024
Document Sponsor (Job Title)	BSW ICB Executive Director of Planning and Performance
Document Manager (Job Title)	BSW ICB Information Governance and Assurance Manager
Document developed in consultation with	SCW CSU IG consultant BSW Information Governance Steering Group
Intranet Location	Insert the location of the document on the intranet
Website Location	Insert the location of the document on the ICB website (if applicable)
Keywords (for website/intranet uploading)	Information governance, IT, data protection

BSW ICB Information Governance Framework

Review Log

Version Number	Review Date (date when approval was given)	Name of reviewer	Approval Process	Reason for amendments

1	09/04/2020		IGSG review Jan 2020
			BSW CCG Governing Body approval 09/04/2020
				Addition of IAO/IAA nomination letters & ToR;
				Addition of TNA;
				Addition of IG Decision Log

1.1	10/03/2021		BSW CCG IGSG	Removal of formal appointment for IAO/IAA, update to TNA V3 & Minor changes
2	06/05/2021		BSW CCG Finance Committee	No amendments; annual review
2.1	April 2022		BSW CCG IGSG	Minor changes: ref to Internal Audit; update to TNA
3	01/07/2022		BSW ICB Board approval 01/07/2022	Adoption of framework for BSW ICB purposes
4	16/03/2023	Susannah Long	BSW IGSG review 14/01/2023 BSW ICB Board approval 16/03/2023	regular review; updates reflect establishment of BSW ICB, updated remit of IGSG and its reporting to BSW ICB Audit Committee, current legal / regulatory environment

BSW ICB Information Governance Framework

Summary of Policy

The information governance framework and its associated policies give clarity and context for BSW ICB information governance activities.

The Information Governance Steering Group is the primary group with oversight and management responsibilities for information governance within BSW ICB. IGSG is chaired by SIRO and attended by the Caldicott Guardian and Data Protection Officer. The IGSG reports to the Audit Committee.

The Information Governance Steering Group leads on the programme for management of information governance and monitoring of activities, arrangements and progress.

The ICB completes a self-assessment against the Data Security and Protection (DSP) Toolkit on an annual basis which is signed off by the ICB before submission to NHS Digital.

The ICB has relevant policies in place to support information governance.

Information Asset Owners (IAO) and Information Asset Administrators (IAA) have specific duties within the ICB to support the information governance arrangements and champion behaviours (Terms of Reference appended, and detailed further in the IAO/IAA IG Handbook)

The ICB has registers of data flows and information assets.

All colleagues are required to complete training in accordance with the Training Needs Analysis (TNA) which as a minimum is annual completion of the Data Security Awareness training available through ConsultOD.

BSW ICB Information Governance Framework

Contents

INTRODUCTION & PURPOSE

1. This framework sets out the approach taken within BaNES, Swindon and Wiltshire (BSW) ICB for embedding information governance and details the continuous improvements that BSW is working towards. The organisation must have a robust information governance management framework to provide the clarity and context for its information governance activities.

2. The framework identifies how BSW will deliver its strategic information governance responsibilities by identifying the accountability structure, processes, interrelated policies, procedures, improvement plans, reporting hierarchy and training within the organisation. BSW will also ensure that the future management and protection of organisational information is in compliance with legislative and Government process and procedure including the NHS Digital 10 Data Security Standards.

SCOPE

3. This document applies to all directly and indirectly employed colleagues within BSW ICB and other persons working within or on behalf of the organisation. This document applies to all third-party contractors or those with similar relationships through their contractual agreement with the organisation.

4. ‘Information governance’ describes the approach taken within which information standards are developed, implemented and maintained by the organisation and ensures best practice applies, in particular to all information relating to the organisation and individuals.

5. Information governance management ensures that data is sourced, held and used legally, securely, efficiently and effectively, in order to deliver the best possible care in compliance with legislation and advice received from bodies including NHS Digital. Information is a vital asset to the organisation supporting the effective management of commissioned services and resources. Therefore, it is essential that all organisational information be managed effectively within a robust information governance management framework.

6. The organisation requires accurate, timely and relevant information to enable it to commission the highest quality healthcare and to operate effectively and meet its objectives. It is the responsibility of all colleagues to ensure that information is accurate and current and is used proactively in the conduct of its business. Accurate information that is dependable plays a key role in both corporate and clinical governance, strategic risk, performance management and service planning.

DEFINITIONS

7. In order to assist colleagues with understanding their responsibilities under this framework, the following types of information and their definitions are applicable:

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('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.
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life.
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially Confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to BSW ICB or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

PROCESS

Implementation objectives

8. To develop information quality assurance standards in alignment with the content of this framework to support:
   - Corporate governance (which ensures organisations achieve their business objectives and meet integrity and accountability standards);
   - Clinical governance (ensuring continuous improvements in the quality of healthcare);
   - Research governance (which ensures compliance with ethical standards).

9. The strategic implementation of this framework will promote continuous improvements in information handling underpinned by clear standards. BSW will be able to ensure that all colleagues manage personal information in compliance with NHS Digital regulations for governance.

10. Colleagues will be aware that their records will not be disclosed inappropriately, which will lead to greater confidence in NHS working practices.

11. The information governance framework should be seen as a tool that will aid the organisation in embedding a 'robust governance framework'. Information governance contributes to other standards by ensuring that data required to support decisions, processes and procedures is accurate, available and endures.

Reporting

12. The Information Governance Steering Group (IGSG) reports to the BSW ICB Audit and Risk Committee; the IGSG Terms of Reference detail the group's responsibilities, remit and membership. The IGSG will present a report to the BSW ICB Audit and Risk Committee, usually in quarter one of each year, including details of the annual Data Security and Protection Toolkit self-assessment submission, an annual report of its activities, and a high-level workplan for the year.

13. Per its oversight function, the IGSG will receive updates on progress with information governance audits, training and toolkit evidence requirements, Data Protection Impact Assessments (DPIA), IG incidents that may have occurred, and will take decisions on information governance issues within its remit and authority. The group will also identify any associated resource implications incurred by the implementation of the information governance framework across BSW ICB governance information activities, bringing this to the attention of the Audit Committee where resource implications pose a significant risk.

14. Any internal audit of information governance shall be reported to the Audit Committee together with any recommendations identified and the associated improvement plans.

15. Minutes of IGSG will routinely be presented to the Audit Committee.

Improvement programme

16. Risks and issues will be identified where they may impact upon delivery of the IG improvement programme which will be monitored by the IGSG.

17. Implementation of robust information governance arrangements will deliver improvements in information handling by following the Department of Health standards (known as the 'HORUS' model), these standards require that information will be:

    Held securely and confidentially

Obtained fairly and efficiently
Recorded accurately and reliably
Used effectively and ethically
Shared appropriately and lawfully

18. Information governance is a framework to provide consistency and best practice for the many different information handling requests and associated guidance. These principles are equally supported by the Caldicott Principles which have been subsumed into the NHS Code of Confidentiality.

19. There are five interlinked principles, which serve to guide these information governance responsibilities:
    - Openness
    - Legal compliance
    - Information security
    - Quality assurance
    - Proactive use of information.

20. Where it is necessary to make a high-level decision regarding the acquiring, processing, sharing, storage or deletion of information outside the DPIA process, Caldicott Guardian, SIRO and DPO will record their decision(s) in the IG Decision Log (Appendix 4).

ROLES & RESPONSIBILITIES

Accountable Officer

21. The Accountable Officer is the 'information governance lead' and has overall responsibility for compliance with information governance legislation and best practices, and the requirements within the 'Data Security & Protection toolkit' (DSPT). The Accountable Officer is responsible for the overall management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information governance is the key to supporting this within the organisation.

Senior Information Risk Owner (SIRO)

22. The SIRO is a member of the Executive Management Team, chairs the Information Governance Steering Group and is accountable to the Audit Committee for the use of information. They ensure that the organisation conducts its business in an open, honest and secure manner, updating the Audit Committee in respect to the annual report, the statement of internal controls and any changes in the law or potential risks. The SIRO is supported by the Caldicott Guardian, the Deputy SIRO, and the Information Asset Owners (IAO).

Caldicott Guardian

23. The Caldicott Guardian is a member of the Executive Management Team and a senior

health or social care professional with responsibility for promoting clinical governance or equivalent functions. The Caldicott Guardian, acting as the conscience of the organisation, plays a key role in ensuring that the organisation satisfies the highest practical standards for handling patient/colleague identifiable information. The Caldicott Guardian is supported by the Deputy Caldicott Guardian.

Data Protection Officer (DPO)

24. This role has the responsibilities as set out in the GDPR. The Data Protection Officer (DPO) reports directly to the ICB Board in matters relating to data protection assurance and compliance, without prior oversight by their line manager. The DPO must ensure that their responsibilities are not influenced in any way and should a potential conflict of interest arise, report this to the highest management level.

25. Their primary duties are to:

- Inform and advise the organisation and colleagues of their IG responsibilities;
- Monitor compliance with the GDPR and the DPA 2018;
- Provide advice, where requested, regarding the Data Protection Impact Assessment, and monitor performance;
- Cooperate with the supervisory authority;
- Be the contact point with the Information Commissioners Office;
- Ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects that the ICO is informed no later than 72 hours after the organisation becomes aware of the incident.

26. They must give due regard to the risks associated with the processing of data undertaken by the organisation and work with the SIRO and Caldicott Guardian to achieve this.

Information asset owners (IAO)

27. Within BSW, IAO are senior colleagues who are owners of one or more identified information assets or data flows of the organisation (Terms of Reference at Appendix 3). There are IAO working in a variety of senior roles to support the SIRO by recording and risk assessing their assets in order to:

- Provide assurance to the SIRO on the security and use of these assets through contribution to the DSPT and an annual report;
- Understand and address risks to the information assets and flows that they ‘own’ facilitated by the completion and ongoing management of DPIA;
- Ensure that appropriate Data Sharing Agreements and/or Data Processing Agreements are in place.
- Ensure that IG Spot Checks and Confidentiality & Safe Haven Audits are completed on an annual basis
- Ensure Consent Checklists are completed to record where consent is relied upon under UK GDPR or under Common Law Duty of Confidentiality
- Ensure that appropriate Data Sharing Agreements and/or Data Processing Agreements are in place.

Information Asset Administrator (IAA)II

28. Within BSW, IAA are colleagues who assist IAO in the management of their Information Assets (Terms of Reference at Appendix 3). IAA serve as local records managers and are responsible for assisting in the co-ordination of all aspects of information governance requests in the execution of their duties, which include:

    - providing support to their IAO;
    - ensuring that policies and procedures are followed locally;
    - recognising potential or actual IG security incidents;
    - undertaking relevant IG audit tasks;
    - consulting their IAO on incident management;
    - ensuring that data flow maps and information asset registers are accurate and maintained.

BSW Information Governance Team

29. The Team manages IG transactional and development arrangements for BSW ICB.

SCW CSU Information Governance service

30. SCW provides IG support services in line with the information governance service specification under any Service Level Agreement for IG Services to customers.
    The SCW CSU Senior IG Consultant, IG Consultant and Senior IG Officer will undertake all operational activities in support of the Service Level Agreement.

The Information Governance Steering Group (IGSG)

31. Reports to the BSW ICB Audit and Risk Committee. Provides assurance to the Committee on the ICB's compliance with information governance legislation / regulation / guidance, national and organisational requirements and standards, and good practice; and on the effectiveness of information governance mechanisms and processes that are in place in the ICB. Provides oversight of information governance arrangements within the BSW ICB and develops and drives the ICB's information governance agenda.

TRAINING

32. It is the responsibility of the organisation to ensure that all new colleagues are provided with information governance, information security, freedom of information and records management training as part of their induction. The Information Governance Handbook is issued upon notification of a new starter. Requirements for initial and ongoing IG training, which is periodically reviewed by the IGSG, is detailed in Appendix 2 to this document and from the latest Training Needs Analysis available on the intranet.

33. All new colleagues must use the NHS Digital E-Learning for Health (e-fh) online IG training tool: nhsdigital.e-lfh.org.uk to undertake the Data Security Awareness training and they will

generally access this through the ConsultOD learning and development portal.

34. This on-line training must be undertaken annually on expiry of their certification.

35. BSW, through its learning and development commitment ensures that appropriate annual training is made available to colleagues and completed as necessary to support their duties. In addition to the Data Security Awareness annual training all IAO, all IAA, the DPO, the Caldicott Guardian and SIRO are required to have undertaken any additional training associated with their identified roles as detailed in the BSW IG Training Needs Analysis (TNA) Protocol (Appendix 2).

36. Following an incident, further training may be delivered as a mandatory requirement. Disciplinary procedures may be used where it is proven that a colleague has acted in breach of the terms of their contract.

EQUALITY IMPACT ASSESSMENT

37. An Equality Impact Assessment (EIA) has been completed for this framework and no significant issues were identified.

MONITORING EFFECTIVENESS

38. The performance of the framework will be monitored in two ways:

- Against the criteria set in the Data Security and Protection Toolkit, using the annual submission on 30 June (or alternative dates as notified) and associated improvement plan.
- The internal audit process and subsequent report to the Audit Committee.

REVIEW

39. This document is reviewed annually unless organisational changes, legislation or guidance prompt an earlier review. Recurrent instances of non-compliance will be investigated to ascertain the source of non-compliance. If it is found that the policy itself is a source of non-compliance, e.g. is not sufficiently clear, this will trigger a review also.

REFERENCES AND LINKS TO OTHER DOCUMENTS

Legislation

40. All colleagues are required to comply with Data Protection Legislation. This includes:

- the General Data Protection Regulations (GDPR); UK GDPR in most circumstance, but may have to comply with EU GDPR (2018) also if operating in both UK and EU;
- the Data Protection Act (DPA) 2018;
- the Freedom of Information Act (FOIA) 2000;

- the Access to Health Records Act (AHRA) 1990;
- the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

41. In addition, consideration will also be given to all applicable law concerning privacy confidentiality, the processing and sharing of personal data including:

- the Human Rights Act 1998;
- the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015 and subsequent amendments;
- the common law duty of confidentiality; and
- the Privacy and Electronic Communications (EC Directive) Regulations.

42. Consideration must also be given to the:

- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse);
- Copyright, Designs and Patents Act 1988;
- Regulation of Investigatory Powers Act 2000;
- Electronic Communications Act 2000;
- Other relevant Health and Social Care Acts;
- Fraud Act 2006;
- Bribery Act 2010;
- Criminal Justice and Immigration Act 2008;
- Equality Act 2010;
- Civil Contingencies Act 2004;
- Terrorism Act 2006;
- Malicious Communications Act 1988;
- Counter-Terrorism and Security Act 2015;
- Digital Economy Act 2010 and 2017.

Guidance

- ICO Guidance
- Dept. of Health and Social Care 2017/18 Data Security and Protection Requirements
- Data Security and Protection Toolkit
- Records management: Code of Practice for Health & Social care
- Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK
- Confidentiality: NHS Code of Practice - supplementary guidance
- NHSX Information Governance

Other documents

43. BSW ICB policies associated with the BSW Information Governance Framework:

- **Confidentiality and Safe Haven Policy**

  This document describes the organisational policy on data protection and confidentiality together with colleagues' responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and on computers. This policy also aims to ensure that the organisation operates procedures to safeguard the privacy and confidentiality of information by ensuring that information sent to or from the organisation is handled in such a way as to minimise the risk of inappropriate access or disclosure.

- **Individual Rights Policy**

  This document details how the organisation will handle requests for personal information including health records for living persons (Subject Access Request), deceased persons (Access to Records) and colleague employment records, as well as the other rights under the GDPR. This policy will be accompanied by a standard operating procedure to support colleagues in processing such requests.

- **Information Security Policy**

  The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient and colleague records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

- **Records Management Policy**

  This policy is written to give the organisation clear information and a records management framework, which includes advice and guidance on all aspects of records management and data quality to inform colleagues of their operational and legal responsibilities.

- **Acceptable Use of IT Policy**

  BSW recognises the need to secure its data, protect its colleagues and patients and have strict control over data in transit. This policy describes how we must use our IT systems and equipment to communicate both internally and externally in a safe, consistent and professional manner.

- **Data Quality Policy**

  BSW ICB recognises that all its decisions, whether clinical, managerial or financial need to be based on information which is of the highest quality. Data quality is crucial and the availability of complete, accurate and timely data is important in supporting patient care, clinical governance, management and service agreements for healthcare planning and accountability.

- **Freedom of Information Policy**

  This policy outlines the organisation's responsibilities in complying with the Freedom of Information Act (2000), the Environmental Information Regulations (2004), the Re-use of Public Sector Information and the relation to the Data Protection Legislation. This policy is a statement of what the organisation intends to do to ensure and maintain compliance with the Act and regulations. It is not a statement of how compliance will be achieved; this will be a matter for operational procedures.

- **Management of Vexatious Applicants Policy**

  This policy aims to provide colleagues with a clear and fair process for dealing with situations where an applicant under FOI or Individual Rights might be considered to be a persistent, habitual, prolific or vexatious applicant and to recommend agreed ways of handling those situations.

- **Risk Stratification Policy**

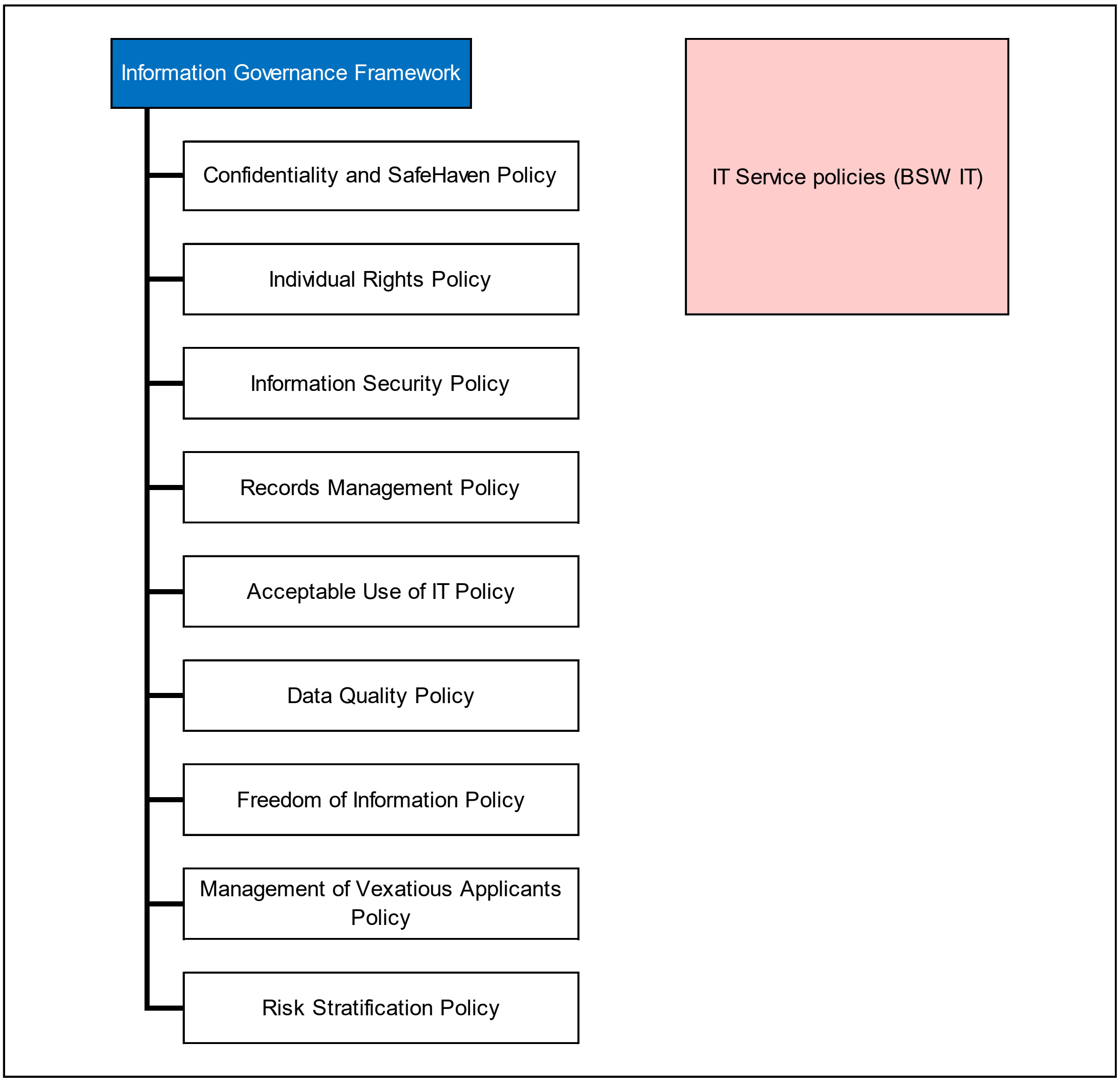
  Risk stratification tools use relationships in historic population data to estimate the use of health care services for each member of a population. This policy provides detail of the principles by which the ICB will utilise risk stratification within the ICS.

- **IT Services Policies**

  IT services provide and support the information systems and networks used by the organisation. IT services are currently provided by SCW CSU and BSW IT. This includes a suite of policies covering various aspects of IT and information security.

APPENDICES

A – BSW Information Governance Framework and associated policies at a glance


Information Governance Framework
Confidentiality and SafeHaven Policy
Individual Rights Policy
Information Security Policy
Records Management Policy
Acceptable Use of IT Policy
Data Quality Policy
Freedom of Information Policy
Management of Vexatious Applicants Policy
Risk Stratification Policy
IT Service policies (BSW IT)

B – Training Needs Analysis Protocol: Information Governance

1. Introduction and purpose

BaNES, Swindon and Wiltshire Integrated Care Board (BSW ICB) must ensure and demonstrate that information is used legally and ethically in line with Data Protection legislation.

The Department of Health has mandated that, as part of the NHS Digital Data Security and Protection Toolkit (DSPT), all relevant NHS staff complete annual Information Governance (Data Security Awareness) training. It is also prudent to ensure that colleagues with key information governance roles have appropriate training.

This document details:

- BSW colleague training requirements; and
- BSW monitoring and reporting arrangements.

2. Scope

This protocol applies to all BSW colleagues, including members of the Governing Body and contracted/non-contracted, honorary, secondments, agency, students, volunteers, interim and temporary colleagues.

3. Training Needs Analysis (TNA)

Full detail of training is available in the Training Needs Analysis (TNA) on the BSW intranet.

3.1 Standard training

Annual Data Security Awareness training is a mandated requirement of the DSP Toolkit. This must be completed by all individuals in scope for this protocol (see above). Line Managers must ensure that all individuals working within their teams are registered with ConsultOD, which is part of NHS South, Central and West Commissioning Support Unit (SCW CSU). Registration is undertaken by completing the form available on the ConsultOD home page.
Existing colleagues are asked to complete their Data Security Awareness Level 1 training annually on expiration of their training certificate. New starters must complete the training within their first week.

> The Data Security Awareness training is accessed via www.consultod.co.uk\ .

The Senior Information Risk Officer (SIRO) and the Caldicott Guardian (CG) and their deputies are key roles for Information Governance and require appropriate training.

The BSW Data Protection Officer (DPO) is a role established by the GDPR and must have suitable and sufficient knowledge and experience to provide independent advice and challenge within the organisation. To facilitate this, the DPO must undertake specialist data protection training and refresh this training on at least a three yearly basis to ensure that their knowledge is up to date.

BSW relies on the Information Asset Owners (IAO) and Information Asset Administrators (IAA) to support the Information Governance Framework within the ICB. IAO and IAA will be offered annual training regarding their duties provided by South Central and West Commissioning Support Unit (SCW CSU).

The BSW Head of Risk Management and Information Governance supported by the BSW Information Governance and Assurance Manager will manage information governance and records management arrangements on a day-to-day basis. In addition to the Data Security Awareness training, and the SCW CSU IAO and IAA training above, they will be expected to undertake such training as is required by their Personal Development Plan to equip them to achieve their objectives.

3.2 Additional training available

The organisation will be made aware of any additional training requirements or opportunities and will consider this for BSW colleagues.

3.3 Reactive training

Where a security breach or a serious incident involving information assets has taken place SIRO, supported by the Information Governance Steering Group (IGSG) may deem it necessary that additional Information Governance training is undertaken by relevant colleagues. This training may be simply the repeat of the Data Security Awareness training or may involve input from SCW CSU.

4. Monitoring and reporting arrangements

The IGSG will, on at least a quarterly basis, receive a report detailing colleague compliance with the Data Security Awareness training. SIRO, on behalf of IGSG, will contact IAO to draw their attention to non-compliance of their team members.

Colleagues persistently failing to complete their Data Security Awareness training may have access revoked to BSW systems at the discretion of the SIRO.

It is important that line managers contact ConsultOD to close accounts of colleagues who have left the organisation to avoid errors in the compliance reporting.

Contact scwcsu.consultod@nhs.net to remove colleagues who have left BSW employment.

A compliance report will be generated as close as possible to the Data Security and Protection Toolkit (DSPT) submission date as evidence for the Toolkit and to inform the final submission figure.

Other training identified within the TNA will support the DSPT submission. DPO, SIRO and CG (and deputies) will be expected to provide training certificates as evidence of successful training completion.

C – BSW ICB Information Asset Owner (IAO) Terms of Reference

The responsibilities of Information Asset Administrators (IAA) fall into four main categories:

Culture

- Positively promote a culture that values, protects and uses information as a strategic asset for the organisation and for public good;
- Regularly discuss Information Governance at team meetings sharing promotional materials where available;
- Play an active role in the development of IG campaigns across BSW;
- Champion best practices to help ensure colleagues understand the importance of effective data security and protection; and
- Exchange methods and good practice with other IAA.

Compliance

- Keep up to date with policy development and where possible contribute to the process to ensure that any gap between policy and practice is closed;
- Participate in the collating of evidence for the DSP Toolkit for the team;
- Ensure team members undertake appropriate Data Protection Impact Assessments (DPIA) before embarking on any project, scheme or development;
- Monitor team members completion of mandatory and recommended IG training;
- Process requests made by SCW CSU to meet data subject rights under the GDPR (DSAR and FOI) and in line with the BSW Individual Rights Policy;
- Assist colleagues to seek permission from their IAO to transfer personal and sensitive information; and
- Process requests for folder access and new folders in the file structure.

Understanding assets and information flows

- Maintain an understanding of all ‘owned’ Information Assets (IA) and how they are used;
- Keep the Information Asset Register (IR) and Data Flow Map (DFM) up to date;
- Serving as local records managers ensuring the accurate storage and retention of records and their content;
- Identify and record information assets for disposal in line with the Records Management Policy – Retention & Disposal Schedule;

Addressing risks

- Raising areas of concern at team meetings or directly with the IAO;
- Auditing compliance where directed;
- Seeking advice from data security and protection subject matter experts in a timely manner.

Please refer to BSW IAO/IAA IG Handbook for further detail.