NHS
Bristol, North Somerset and South Gloucestershire
Clinical Commissioning Group

70 YEARS OF THE NHS 1948 - 2018

Meeting of Governing Body

Date: Tuesday 7th August 2018
Time: 1.30pm
Location: Clevedon Hall, Elton Rd, Clevedon, North Somerset, BS21 7RQ

Agenda number: 10.4

Report title: Information Governance Compliance, Data Security and Protection Toolkit and Information Governance Policies

Report Author: Caroline Dominey-Strange, IG Manager
Report Sponsor: Sarah Truelove, Chief Finance Officer and Senior Information Risk Owner

1. Purpose

To provide an update on Information Governance compliance and assurance of the Information Governance programme for the year ahead.
To obtain approval of the Information Governance Policy and the Confidentiality and Security of Information Policy which outline the CCGs approach to Information Governance.

2. Recommendations

The Governing Body is asked to note:

- The Information Governance Compliance and the Data Security and Protection Toolkit Briefing

The Governing Body is asked to approve:

- The Information Governance Policy
- The Confidentiality and Security of Information Policy

3. Executive Summary

The CCG is committed to managing information securely and confidentially. There are new and updated requirements under a new Data Security and Protection Toolkit and updated legislation, an Information Governance Workplan has been developed for the year ahead to provide assurance of ongoing compliance.

In addition the Information Governance Policy and Confidentiality and Security of Information Policy are provided as part of a suite of Information Governance (IG) policies which have been updated to align to the new General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018. All staff are responsible for ensuring good Information Governance, these polices provide the framework and principles which all staff must follow to support compliance.

4. Financial resource implications

There are no financial resource implications to this. However, failure to comply with relevant Data Protection legislation can result in significant fines to the organisation.

5. Legal implications

The workplan and policies support the CCGs compliance with General Data Protection Regulation (GDPR) and Data protection Act 2018.

6. Risk implications

If the plan and policies are not adopted or implemented there is a risk of non-compliance with data protection legislation resulting is damage to individuals privacy, breach of confidentiality and potential action (including significant fines) against the organisation.

7. Implications for health inequalities

There are no implications for health inequalities.

8. Implications for equalities (Black and Other Minority Ethnic/Disability/Age Issues)

The Equality Impact Screening Assessment has deemed that a full Assessment is not required.

9. Implications for Public Involvement

There has been no public involvement in the creation of these policies which are aimed at ensuring data protection legislation is reflected in CCG policy.

Agenda item: 10.4.1

Report title: Information Governance Compliance and the Data Security and Protection Toolkit

1. Background

Information Governance Assurance is provided through compliance with relevant legislation such as the General Data Protection Regulation 2016 (GDPR) and through the use of the Information Governance Toolkit. Historically, all organisations that accessed patient data were required to complete the annual Information Governance Toolkit assessment.

This toolkit has now been replaced by a new Data Security and Protection Toolkit (DSPT), coupled with the recent changes in Data Protection legislation the Clinical Commissioning Group (CCG) is now operating under a new framework of Information Governance (IG). This briefing outlines the changed requirements, how they impact the CCG and identify the next steps to ensure continued compliance.

2. Toolkit Submissions

The three predecessor CCGs have demonstrated IG assurance through the IG Toolkit obtaining year on year improvements, as detailed below.

	2015/16	2016/17	2017/18
BCCG	**78%**	**80%**	**82%**
SGCCG	**77%**	**81%**	**81%**
NSCCG	**78%**	**82%**	**82%**

The aspiration is for BNSSG to continue this trajectory and demonstrate a high and improving level of Information Governance compliance. The DSPT will be the principle method to evidence this.

3. Background to the Data Security & Protection Toolkit

The new toolkit is a self-assessment of information governance and security compliance and has been designed to be user-friendly and reduce duplication.

The toolkit is structured around the 10 Data Security standards identified by the National Data Guardian. A detailed explanation of each standard is available in the Data Security Standards Guide[1]. Each standard is split into a number of assertions for which the CCG is required to identify evidence. The evidence is either mandatory or not, the CCG must provide all the mandatory evidence to be able to successfully complete the DSPT.

Toolkit compliance is no longer assessed by levels or percentages an organisation is compliant if they have met all mandatory evidence requirements. Therefore, to demonstrate year on year

[1] https://www.dsptoolkit.nhs.uk/Help/2

improvements the CCG will rely on an assessment of the evidence used and any internal audits completed. It is proposed that the CCG aim to meet all mandatory and non-mandatory requirements to provide the highest level of assurance.

There are three versions of the toolkit for different organisation types: Large, Small or GPs. The CCG is classified as a Small organisation this removes some of the evidence requirements compared to a Large organisation.

4. Approach to ensuring Information Governance Compliance

An Information Governance workplan is included in Appendix 1, this outlines the principle Information Governance (IG) activities required over the coming year to support the CCGs IG activities, compliance with new GDPR legislation and the requirements of the DSPT. The workplan will be updated quarterly to demonstrate progress. Key activities are identified below.

Policy Review

Continued review of the CCGS Information Governance and Security policies and procedures is required to ensure compliance with GDPR and DSPT. This includes further review of privacy notices and transparency information which is provided to the public and patients regarding how we use their information.

Staff survey

The DSPT requires the results of a Staff Survey to be included as evidence, the toolkit provides 17 questions to be asked of staff and the CCG must provide the percentage of staff who agree or strongly agree with each of the statements to assess their understanding and awareness of Information Governance and Security

IT and Cyber Security

The DSPT now has a significant proportion of Information Security and IT related assertions, this is a reflection of the toolkit being aligned to the National Data Guardian standards. The toolkit is designed so that organisations who confirm:

- that they only use NHS mail
- are fully covered by Cyber Essentials Plus accreditation or
- meet ISO27001 security standard

are exempt from being required to provide a number of evidence requirements which will be automatically marked as complete, since the accreditation itself provides the required evidence. The CCG will work closely with SCW as IT service provider to ensure that these evidence requirements are fully met.

IAO Activities

The activities of Information Asset Owners and Administrators are becoming increasingly important for both DSPT and GDPR compliance. Completion of Information Asset Registers and Data Flow maps which are aligned to GDPR is a requirement these registers must be fully completed, maintained and appropriately approved. The CCG must be assured that any Data Processors who provide services on behalf of the CCG are GDPR compliant and that appropriate contracts are in place with all suppliers; this activity will be supported by Information Asset Owners.

The role of Information Asset Owner is of increasing importance for the CCG and it is proposed that training and regular meetings are held with IAOs to ensure they are fully equipped and supported; this will also provide a forum for organisational oversight of IG activities.

Audits and Process Reviews
Audits and spot checks continue to be important to provide evidence and assurance of good practice. Where certain processes are known to be problematic, high risk or prone to Information Governance incidents there is a requirement to evidence that process reviews have taken place and recommendations made.

Training
The Information Governance training requirement remains at 95%, it has been agreed that staff should complete their IG training by December 2018 regardless of when it expires. This means that only new members of staff will be required to complete between January and March and will eliminate the need to spend significant resource in ensuring that staff are up to date during March where staff are busy with other end of year processes.

Incident Reporting Tool
The toolkit provides an incident reporting tool, the tool along with the published guidance has been updated to align to GDPR. Information governance incidents are now to be assessed according to the impact to the rights of freedoms on individuals. This means that we must assess incidents according to the potential adverse impact on the individual and the likelihood of that adverse impacts occurring. Incidents meeting the reporting threshold will be reported through the DSPT to the Information Commissioners Office and where required to the Department for Health and Social care.

5. Monitoring Progress

Organisations are able to submit their DSPT at any time during the year (April – March) and may submit multiple times should they wish to update evidence. As a new organisation BNSSG CCG does not have a current toolkit submission (the three previous organisations each submitted separately). Clarification is being sought as to when BNSSG must make its first submission as a new organisation, but will either be in October 2018 or March 2019. However the process of collecting the required evidence and strengthening IG processes will commence immediately.

Progress against the IG workplan will be reported quarterly.

6. Financial resource implications

There are no financial resource implications to this. However, failure to comply with relevant Data Protection legislation can result in significant fines to the organisation.

7. Legal implications

This approach to Information Governance supports the CCGs compliance with General Data Protection Regulation (GDPR) and Data Protection Act 2018.

8. Risk implications

If this approach is not implemented there is a risk of non-compliance with data protection legislation resulting is damage to individuals privacy, breach of confidentiality and potential action (including significant fines) against the organisation.

9. Implications for health inequalities

There are no implications for health inequalities.

10. Implications for equalities (Black and Other Minority Ethnic/Disability/Age Issues)

There are no implications for inequalities.

11. Recommendations

1. To note the requirement to achieve all mandatory requirements of the DSP
2. To note the aspiration to achieve all non-mandatory requirements of the DSP
3. To note the IG Workplan and a means to monitor and review progress

Report Author: Caroline Dominey-Strange, Information Governance Manager
Report Sponsor:

Appendix 1 – 2018/19 Information Governance Improvement Plan – updated June 2018

Workplan for 2018/19 Version 1.0_June 2018

Action		Detail	Q1	Q 2	Q 3	Q 4	Link to DSP Requirements
IG Governance Activities	Draft and Agree Workplan	Create and finalise IG work plan; to be approved by customer.	Submitted				
	Quarterly Reports	To provide quarterly IG update reports to the IG Committee and/or SIRO/Caldicott Guardian and DPO	Submitted				
	Annual Information Risk Report	To provide an annual Information Risk update report to the IG Committee and/or SIRO and Caldicott Guardian					
	IG Committee Support	To attend and support customer IG Committees or similar	Complete for Q1				
DSP Toolkit	Review of Data Security and Protection (DSP)Toolkit	Detailed review of the new Data Security and Protection Toolkit; additional items to be added to workplan as required	Submitted				
	Implementation of Staff Survey	DSP provide 17 survey questions to be used to assess staff awareness and engagement	Discussed in report				1.1.5; 1.2.5; 1.2.6; 1.5.4; 2.2.1; 2.2.2; 2.2.3; 2.2.4; 2.3.3; 2.3.4; 2.3.5; 3.2.1;

							4.2.3; 6.2.3; 6.4.3; 6.4.4; 7.1.3
	Information disposal contracts	Review of contract					1.8.3
	Review of Employment Contracts	To ensure inclusion of relevant clauses. To also evidence that the organisation holds list of staff and roles					2.3.2; 4.1.1
	Business Continuity & Data Security Incident Management plan	To support customer in identifying DSP requirements					7.1.1; 7.1.2; 7.1.4; 7.2.1; 7.2.2; 7.2.3; 7.2.4; 7.2.5; 7.2.6; 7.2.7; 7.2.8; 7.2.9; 7.2.10
	Support of DSP Toolkit	Support to be spread across the year.					
IG Policy & Procedures	Policy Review	To review policies, strategy and procedures and ensure re-approval where required. To include the full suite of policies required for the DSP including Data Quality, Records Management. To ensure GDPR is covered.	IG Policy, Confidentiality Policy submitted to Policy Review Group				1.1.2; 1.2.1; 1.2.2; 1.2.3; 1.2.4; 1.7.1; 1.8.1; 1.8.2
	Fair Processing Notice Review	This has been updated for GDPR but required continuous review	Further support to be provided				1.3.2; 1.3.3
	Access to information requests	Review of SAR policy to ensure compliance with GDPR and report on handling of requests to include FoI request where					1.3.5; 1.3.6

		relevant. Data to be included in quarterly IG reports					
	Staff procedure about how to provide information about processing and individuals' rights at the correct time.	Review procedures to ensure this DSP requirement is covered and produce documentation if required. To check against SCW GDPR policies.					1.3.4
	Review Staff Guidance	Review all guidance and advice provided to staff to ensure it is up to date, GDPR compliant and fit for purpose. To include implementation of Staff IG Handbook.					1.5.1
	Review of IG Incident reporting	To review internal policy and process for identifying, reporting and managing IG Incidents. To include review of learning that takes place after incident occurs and align to GDPR.					6.1.1; 6.1.2; 6.1.3; 6.1.4; 6.1.5; 6.2.1; 6.2.2; 6.2.4
Information Asset Owners Support and Activities	Information Asset Owner Engagement	To develop Information Asset Owner role and engagement; to implement regular IAO meetings/training.					
	Information Asset Owner handbook	To include guidance on completing spreadsheets					
	Review of Information Asset Register	Annual review - to ensure gaps are filled in. To consider reporting on a quarterly basis.					1.4.4; 2.1.1; 2.1.2; 4.3.4
	Key Information Asset Risk Assessments	To complete detailed risk assessments of key information assets					

	Review of Data Flow Mapping / Information Sharing Audit	Annual review - to ensure gaps are filled in. To consider reporting on a quarterly basis. To be formally approved by SIRO					1.4.1; 1.4.2
	Detailed review of external flows of identifiable data	Review external data flows for information sharing/access agreements, location of data processing etc.					1.4.1
	Detailed review of IG Contract Clauses	Ensure contracts are up to date and GDPR compliant	Ongoing				
	Process Reviews	To review incidents and support customers in reviewing their processes which lead to increased risk.					5.1.1; 5.2.1; 5.3.1; 5.3.2
	Information Sharing Partner - Compliance Review / Information Sharing Audit	Review of information sharing partners and signatories to the overarching Information Sharing agreement, to include review of the overarching agreement					
IT Activities	IT Policies	To review and update IT and IT Security Policies					1.1.2; 1.2.1; 1.2.2; 1.2.3; 1.2.4
	Review of IT Systems and related security measures	To list systems which do not support individual login with the risks outlined and what compensating measures are in place.					1.4.5
	Identify IT Security Controls	Including list of Role Based Access					1.6.3; 4.1.2
	System Administrator Agreements	To ensure that all system administrators have signed an agreement which holds them accountable to the highest standards of use. To ensure IT Administrators activities are logged					4.3.1; 4.3.2

	IT Acceptable Use	To review and update IT AUP To include reference to monitoring					4.3.3; 4.3.5
	IT Evidence for DSP	To engage with IT regarding elements of DSP Toolkit. Where Cyber Essentials Plus accreditation is held it should cover ALL systems.					6.3.1; 6.3.2; 6.3.3; 6.3.4; 6.3.5; 6.4.1; 6.4.2; All of 8, 9 and 10.
	IT Suppliers due diligence	To carry out IG due diligence on IT suppliers to ensure appropriate contracts, governance and security measures are in place					All of 10
National Opt Out Programme	Implementation of the National Opt Out Programme	To review requirements and required actions for the organisation, including updates to Privacy Notices if appropriate					
Education and Communications	IG Communications with staff	Monthly IG Communications to be circulated to staff - to include top tips (i.e. locking screens)	Complete for Q1				
	IG Education activities / TNA Review	To review all aspects of IG training including (Induction, Stat Man, SIRO, CG and IAOs). To ensure records of completion are maintained.	To complete				2.3.1; 3.1.1; 3.1.2; 3.1.3; 3.4.1; 3.4.3; 3.5.1
	Training Compliance	To support the maintenance of a 95% compliance rate (this is still required under the news DSP Toolkit). To include the 'average mark of first attempt'	To complete				3.3.1; 3.3.2
	Training	To provide face to face IG training as required					3.3.1
Audits	Starters & Leavers	To audit IG aspects of starters and leavers processes including the closure of dormant accounts.	Complete for Q1				1.5.2

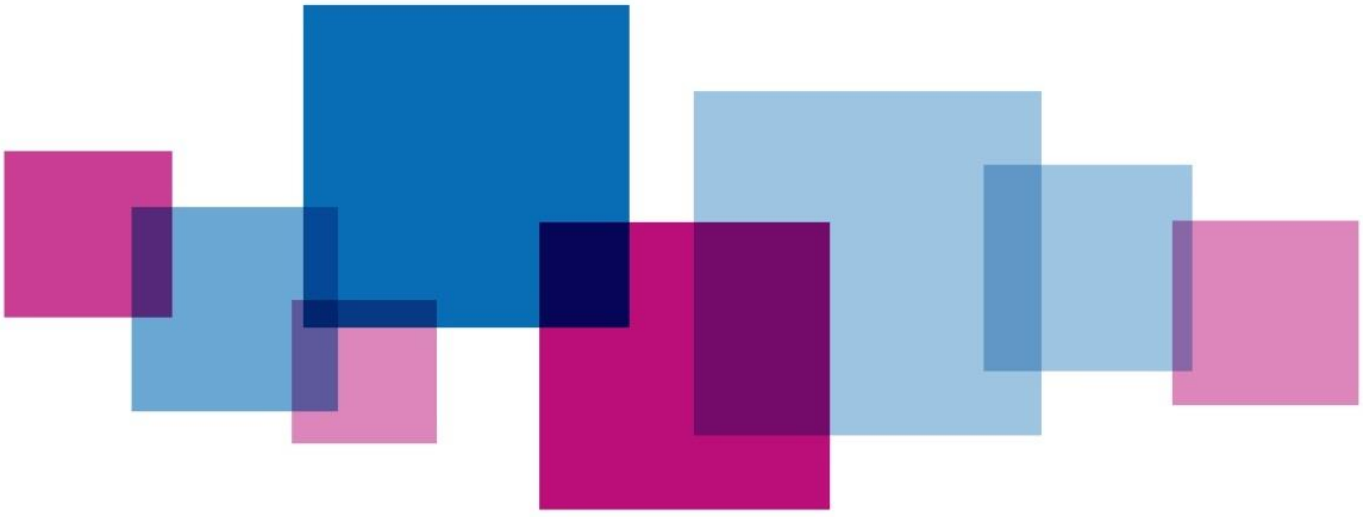
	Smartcard Audit	Audit roles and functions. Review RBAC positions	In progress				1.5.2; 4.2.1
	Site Visits	To audit physical security and implementation of IG processes at identified sites Particular care to be taken during office moves and additional audits where required					1.5.2; 1.5.3; 1.6.4
	Clinical Data Audits	To carry out regular audits of access to clinical data e.g. Connecting Care	Awaiting CC audit data				1.5.2
	Registration Authority Audit	To complete an annual audit of the RA team procedures					1.5.2
	Data Protection Impact Assessments	To ensure policy is up to date and covers Privacy by Design To review and advise on all submitted DPIAs. To review whether DPIAs are required for any existing activities.	Complete for Q1				1.6.1; 1.6.2; 1.6.7; 1.6.8; 1.6.9; 1.6.10; 1.6.11; 1.6.12; 1.6.13
	Internal Audit	To support an Internal Audit of IGT compliance					
	Audit of user accounts	To support the customer on completion of relevant audits To identify incidents relating to miss matched access rights					4.2.1; 4.2.2

	No activity due
	Activity due during quarter

NHS
Bristol, North Somerset and South Gloucestershire
Clinical Commissioning Group

70 YEARS OF THE NHS 1948 - 2018

Information Governance Policy



Shaping better health

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	
Responsible Executive Director:	Sarah Truelove
Author and Job Title:	Information Governance Team, CSU
Date Approved:	
Approved by:	
Date of next review:	June 2020

	Yes/No/NA	**Supporting information**
Has an Equality Impact Assessment Screening been completed?	Yes	
Has the review taken account of latest Guidance/Legislation?	Yes	
Has legal advice been sought?	No	Policy provided by SCW IG Team
Has HR been consulted?	Yes	via Policy Review Group
Have training issues been addressed?	Yes	
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by JCC?	No	
Are there financial issues and have they been addressed?	No	
What engagement has there been with patients/members of the public in preparing this policy?	N/A	
Are there linked policies and procedures?	Yes	
Has the lead Executive Director approved the policy?	Yes	Sarah Truelove to approve after Policy Review Group
Which Committees have assured the policy?		Policy Review Group Governing Body
Has an implementation plan been provided?	Yes	
How will the policy be shared with: • Staff? • Patients? • Public?		Policy will be available via the organisation's website
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	No	

Version Control *please remove this box once approved and finalised*		
Version	**Date**	**Consultation**

Contents

Information Governance Policy

1. Introduction

The role of the CCG is to support the commissioning of healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will uphold the NHS Constitution. This policy is important because it will help the people who work for the CCG to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

2. Purpose and scope

Information is a vital asset. It plays a key part in ensuring the efficient management of service planning, resources and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

Information Governance looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal and confidential information. Without access to information it would be impossible to provide quality healthcare and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

- Information Governance Management
- Confidentiality and Data Protection Legislation assurance
- Corporate Information assurance
- Information Security assurance
- Secondary Use assurance

The aims of this document are to maximise the value of organisational assets by ensuring that information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, the CCG will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met

- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff

The scope of this document covers:

- All permanent employees of the CCG and;
- Staff working on behalf of the CCG (this includes contractors, temporary staff, and secondees).

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard information. The CCG also recognises the need to share information in a controlled manner. The CCG believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents

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 SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

3. Duties and responsibilities

The CCG has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements. The CCG is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Executive Management Team

It is the role of the CCG Executive Management Team to define the CCG policy in respect of Information Governance, taking into account legislative and NHS requirements. The Executive Management Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Information Governance Group

The CCG Information Governance Group is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in the CCG and raising awareness of Information Governance.

All staff have responsibility for complying with this policy and with Data Protection Legislation, the following roles have specific responsibilities:

Accountable Officer

The CCG Accountable Officer has overall responsibility for Information Governance within the organisation. As Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is now required within the Statement of Internal Control which the Accountable Officer is required to sign annually.

Information Risk Owner (SIRO)

The Senior Information Risk Owner for the CCG is an executive board member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at Board level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The SCW Information Governance Manager will support the SIRO in fulfilling this role.

Caldicott Guardian

The Caldicott Guardian is the person within the CCG with overall responsibility for protecting the confidentiality of personal data and special categories of personal data (described as Personal Confidential Data (PCD)) in the Caldicott 2 report, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the CCG Board and relevant committees on confidentiality issues. The SCW Information Governance Manager will support the Caldicott Guardian in fulfilling this role.

Data Protection Officer

The Data Protection Officer (DPO) is the person that has been identified within the CCG that has the responsibilities as set out in the GDPR guidance, such as monitoring compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the and ICO

SCW Information Governance Manager

The SCW Information Governance (IG) Manager supports the CCG DPO in ensuring that the Information Governance programme is implemented throughout the CCG. The IG Manager is also responsible for co-ordinating a number of activities that contribute to the completion and annual submission of the Data Security and Protection Toolkit for the CCG. The IG Manager will support the CCG's SIRO, Caldicott Guardian and DPO in investigating Serious Incidents Requiring Investigation (SIRIs), offer advice and ensure the organisation complies with legislation, policies and protocols as per the SLA.

Information Asset Owners (IAO)

The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The IG Manager will support the IAOs in fulfilling their role.

Data Custodians (DC's)/Information Asset Administrators (IAA's)

This important role is required to support the IAO's and SIRO who will work with the Information Governance Team to ensure staff apply the Data Protection Legislation and Caldicott Principles within working practices. The IG Manager will provide local face to face IG training if required.

4. Definitions of terms used

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents

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: (i) The racial or ethnic origin of the data subject (j) Their political opinions (k) Their religious beliefs or other beliefs of a similar nature (l) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (m)Genetic data (n) Biometric data for the purpose of uniquely identifying a natural person (o) Their physical or mental health or condition (p) 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 SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

5. Legal compliance

The CCG regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.

The CCG will maintain policies to ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

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, the

common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

The CCG, when acting as a Controller, will identify and record a condition for processing, as identified by the GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (e) ' processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller', the CCG will identify the official authority (legal basis) and record this on relevant records of processing.

6. Processes/requirements

The CCG will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).

Non-confidential information about the CCG and its services will be available to the public through a variety of media.

The CCG will maintain policies to ensure compliance with the Freedom of Information Act. Please refer to the Freedom of Information Policy.

The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media. Please refer to the Communications Strategy.

The CCG will maintain clear procedures and arrangements for handling requests for information from the public. Please refer to The CCG Individual Rights Policy in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

The CCG will maintain policies to ensure compliance with the Records Management Code of Practice for Health and Social Care (2016). Please refer to The CCG Records Management Policy.

7. Information security

The CCG will maintain policies for the effective and secure management of its information assets and resources.

The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training. Please refer to the CCG Information Security, Remote Working and Portable Devices and Network Security policies.

The CCG will adhere to the NHS Guidance for reporting, managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner's Office (ICO) must be informed no later than 72 hours after the organisation becomes aware of the incident. Please refer to The CCG Incident Reporting Policy.

8. Information Quality Assurance

The CCG will maintain policies and procedures for information quality assurance and the effective management of records. Please see the CCG Records Management Policy.

The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements.

Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

Wherever possible, information quality should be assured at the point of collection.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

9. Commissioning of new services

The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the CCG SIRO and the Information Asset Owner's.

All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA and where required, seek review from the SCW IG Data Protection Impact Assessment Panel prior to approval or further work.

The CCG will maintain a DPIA framework that includes an approved template, guidance and supporting checklists.

10. Review

This policy must be reviewed annually or as required by law.

11. Training requirements

All new starters to the CCG inclusive of temporary, bank staff and contractors must undertake Information Governance induction training via the ConsultOD portal, to evidence compliance with the Data Protection Legislation and the DSP Toolkit assertions as part of the induction process. Extra training will be given to those dealing with requests for information. A register will be maintained of all staff who have completed the online training and those who have attended face to face training sessions where these are offered.

Annual IG training should be undertaken by all staff via the ConsultOD portal or face to face training.

12. Equality Impact Assessment

Equality Impact Analysis (EIA) screening has been completed and a full assessment is not required. A copy of the EIA screening is attached at Appendix 16.1.

13. Monitoring compliance and effectiveness

This policy will be monitored by the CCG Policy Review Group to ensure any legislative changes that occur before the review date are incorporated.

The CCG IG action plan, along with regular progress reports will be monitored by the CCG Information Governance Group.

Compliance with the Data Security and Protection Toolkit will be assessed by NHS Digital including a review of evidence, as part of the CCG performance assessment.

The CCG will ensure that information governance is part of its annual cycle of internal audit. The results of audits will be reported to the CCG Information Governance Steering Group along with relevant action plans which they will monitor. Reports will also be provided to the Corporate Governance & Assurance Group.

Compliance with the CCG policies is stipulated in staff contracts of employment. If staff members are **unable** to follow the CCG policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with the CCG policies or failure to report non-compliance may be treated as a disciplinary offence.

14. Countering Fraud

The CCG is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document.

15. References, acknowledgements and associated documents

- NHS Digital Codes of Practice
- https://digital.nhs.uk/codes-of-practice-handling-information/confidential-information
- Department of Health Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- CQC Code of Practice
- http://www.cqc.org.uk/sites/default/files/20160906%20Code%20of%20practice%20on%20CPI%202016%20FINAL.pdf
- Health and Social Care (Safety and Quality) Act 2015 http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted
- NHS England Policy https://www.england.nhs.uk/publication/confidentiality-policy/
- All the CCG Policies, procedures and guidance relating to the management and processing of information within the organisation including:
    - Records Management Policy

- Freedom of Information and SARs Policy
- Confidentiality and Security of Information Policy
- Incident Reporting Policy

16. Appendices

16.1. Equality Impact Assessment Screening

Equality Impact Assessment Screening		
Query	**Response**	
What is the aim of the document?	The Information Governance Policy details how the CCG will meet its legal obligations and NHS requirements concerning the management of information and the governance arrangements in place to support this.	
Who is the target audience of the document (which staff groups)?	All staff	
Who is it likely to impact on and how?	Staff	X
	Patients	X
	Visitors	X
	Carers	X
	Other – governors, volunteers etc	X
Does the document affect one group more or less favourably than another based on the 'protected characteristics' in the Equality Act 2010:	Age (younger and older people)	
	Disability (includes physical and sensory impairments, learning disabilities, mental health)	
	Gender (men or women)	
	Pregnancy and maternity	
	Race (includes ethnicity as well as gypsy travellers)	
	Sexual Orientation (lesbian, gay and bisexual people)	
	Transgender people	
	Groups at risk of stigma or social exclusion (e.g. offenders, homeless people)	
	Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)	

16.2. Implementation plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	To have policy available to all staff	To be published on the Hub	Comms/IG	31/07/2018	30/09/2018	Comms team
Staff	To ensure all staff are aware of the policy	To include summary of highlights in The Voice	Comms/IG	31/07/2018	30/09/2018	Comms team

16.3. Policy Statement on Data Definitions

In order to ensure compliance with the new General Data Protection Regulations which came into effect on 25th May 2018 a thorough review and update of SCW Policies, Procedures and Guidance has been undertaken. During the review it was found that there were multiple definitions used to describe personal and sensitive data, with very few policies including business or commercially sensitive data. In order to ensure a consistent use of terminology across the suite of relevant documentation the following definitions and statement were proposed for use:

'Personal Data' as defined by GDPR
'Sensitive Data' to include:

- GDPR "Special Categories" of Personal Data
- Personal Confidential Data (NDG Review)
- Business / Commercially Sensitive Data

The organisation is now clearer as to the terminology to be used in the GDPR and the Data Protection Act 2018, the following amendments are proposed

'Personal Data' as defined by GDPR
'Sensitive Data' to be replaced by **'Special Categories of Personal Data'** as defined by the GDPR
'Commercially Sensitive Data' to be replaced by **'Commercially confidential information'**
'Personal Confidential Data' to be retained but the definition enhanced to describe the considerations needed where 'data owed a duty of confidentiality (under the common law)' is involved and where implicit/explicit consent may be applicable.

The rationale behind this is due to the continued use of 'Sensitive' data within the Data Protection Act 2018 but not in relation to the processing of health data. Categories of data previously considered as 'sensitive' are included as 'Special Categories of Personal Data' with the addition of Genetic and Biometric data. It does not however include information that is processed for the purposes of law enforcement or for the intelligence services as it did previously. These are covered in part 3 and part 4 of the Data Protection Act 2018 as these are Member State derogations not derived from the GDPR.

Under Part 3 – Law enforcement processing, Chapter 2, section 35, subsection 8, the Data Protection Act 2018 refers to 'sensitive processing' and not 'sensitive data'. The categories of data included in what is considered 'sensitive processing' are the same as those defined as 'Special Categories of Personal Data' but it is the act of processing that is defined as sensitive and not the category of data.

Under Part 4 – Intelligence services processing, Chapter 2, section 86, subsection 7, the Data Protection Act 2018 also refers to 'sensitive processing' and not 'sensitive data'. In addition to those categories already recognised as 'Special Categories of Personal Data', it also includes (i) the commission or alleged commission of an offence or (ii) proceedings for an offence, disposal of proceedings or sentence.

Due to the continued use of 'sensitive' as a term but used contextually differently under the new legislation, it is proposed to discontinue use of it except in relation to the processing of data for law enforcement and intelligence services purposes. This is likely to be outside of the majority of

processing activities undertaken by the BNSSG and other health partners as they do not fulfil the criteria of a 'competent authority' as defined in the act.

Definitions to be included in Policies

Personal Data	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	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (q) The racial or ethnic origin of the data subject (r) Their political opinions (s) Their religious beliefs or other beliefs of a similar nature (t) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (u) Genetic data (v) Biometric data for the purpose of uniquely identifying a natural person (w) Their physical or mental health or condition (x) 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 SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.