Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
		Information Governance Strategy
Could this policy be incorporated within an existing policy?	no	It is a requirement of the IG Toolkit to have an IG Strategy
Does this policy follow the style and format of the agreed template?	yes	
Has the front sheet been completed?	yes	
Is there an appropriate review date?	yes	
Does the contents page reflect the body of the document?	yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	yes	Information Governance Toolkit Requirement 130, 131 CQC requirement regulation 17
Are all appendices appropriate and/or applicable?	yes	
Have all appropriate stakeholders been consulted?	yes	To be Ratified by Executive Team
Has an Equality Impact Assessment been undertaken?	yes	
Is there a clear plan for implementation?	yes	Staff to be notified via staff news bulletin
Has the document control sheet been completed?	yes	
Are key references cited and supporting documents referenced?	yes	

|		
Does the document identify which Committee/Group will approve it?	yes	Executive Team
Plans for communicating policy to – staff; practice membership; public (as appropriate)	yes	Staff to be notified via staff news bulletin

Individual Approval

If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

Name	Caroline Hall	Date	08.01.18
Signature			

Committee Approval

If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.

Name	Kathryn Magson	Date	08.01.18
Signature			
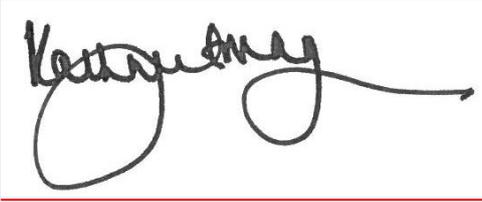
Information Governance Strategy

Version Number	2.0
Ratified By	Executive Team
Date Ratified	January 2018
Approved By	Information Governance Group
Date Approved	07/12/2017
Name of Originator/Author	Ruth Boughton Information Governance Manager
Responsible Director	Caroline Hall
Staff Audience	All staff
Date Issued	January 2018
Next Review Date	January 2019

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
1.0		New document	20/1/2016	Head of Information Governance
1.0		review	May 2016	IG Manager
2.0		Annual Review Changes to reporting from Risk Group to Senior Leaders Team Added reference to new General Data Protection Regulation	November 2017 06/12/2017	IG Manager

1. INTRODUCTION

Information Governance Management Framework is the structure that integrates standards and best practice that apply to the safe and effective processing and protection of information.

The information governance strategy sets out in broad terms the approach and mechanisms, Herts Valleys CCG will use to assure the delivery of a robust Information Governance Framework.

The CCG is committed to achieving a standard of excellence in Information Governance by ensuring information is dealt with legally, securely, efficiently and effectively in the course of CCG business.

2. PURPOSE

The Information Governance Strategy cannot be seen in isolation as information plays a key part in corporate, clinical governance, risk management, performance and business management. This strategy is therefore closely linked with other CCG strategies to ensure integration with all aspects of the CCG's business activities.

There are three key components underpinning this strategy. These are:

- The annual action plan arising from base line assessment against the standards and control set out in the Information Governance Toolkit (IGT).
- The Information Governance Management Framework which outlines how the CCG is addressing the information governance agenda.
- The Information Governance Policy which outlines the objectives for information governance.

The overriding critical success factor for effective IG will be to develop and maintain good management of information governance awareness and practice achieved via effective programme of IG awareness, training and monitoring.

This strategy is applicable to everyone working for the CCG including permanent, temporary and contract staff.

3. ROLES AND RESPONSIBLITIES

Ultimate responsibility for IG lies with the CCG Governing Body. The Governing Body is responsible for ensuring the CCG is able to sign off the statement of compliance with the Information Governance toolkit.

3.1 Roles and Responsibilities within the Organisation

The Chief Executive has overall responsibility and responsibility of for Information Governance.

The Senior Information Risk Owner (SIRO), the Head of IM&T and the Information Governance Manager, have responsibility for overseeing all aspects of information governance. Currently, the SIRO is the Chief Finance Officer.

The Information Asset Owners (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets of the CCG. It is a core IG objective that all Information Assets of the CCG are identified and that the business importance of those assets established.

The Caldicott Guardian is the senior person who is the conscience of the organisation and is the senior person who is responsible for protecting the confidentiality of patient and service user information. The Caldicott Guardian is the Director of Nursing and Quality.

The Information Governance Manager supports the:
- Caldicott Guardian and SIRO.
- The SIRO in relation to reporting, investigating and monitoring Serious Incidents in relation to the requirements set out by HSCIC.
- FOI lead to interpret and apply both the FOI and EIR Acts.

The post holder as specified in relevant policies has responsibility for monitoring, advising on or processing, lawful and procedural requirements relating to applications for personal data under the Data Protection Act.

The CCG will also aim ensure that the new General Data Protection Regulation (GDPR), which replaces the DPA 1998 is implemented within the CCG by May 2018.

Managers must ensure all staff, whether permanent, temporary or contracted and contractors are made aware of their responsibility for ensuring they are aware of the IG requirements incumbent upon them and for ensuring they comply with these on a day- to-day basis.

3.2 Consultation and Communication with Stakeholders

This strategy will be published on the intranet and monitored through the IG Committee.

4. CONTENT

Aim

- To continue monitoring compliance of the IG Toolkit, ensuring that year on year improvement is achieved.
- To develop an action plan for the introduction of the new EU data protection regulations.

Key Priorities for 2017/18

- The CCG will ensure the IG toolkit attainment as a minimum Level 2 (we can do better if we choose to)   That the action plan is completed to ensure that the CCG is General Data Protection Regulation (GDPR) compliant for May 2018 when the new act comes into force.
- The IAOs/IAAs will be fully conversant in their roles and responsibilities ensuring their asset spreadsheets are up to date and risk assessed
- An audit is undertaken to ensure that we have no personal identifiable data following the ceasing of the Accredited Safe Haven
- The IG risk register will be updated regularly ensuring any red risks are flagged to the Senior Leaders Team
- The CCG will ensure at least 95% of staff undertake their annual online IG training.
- HBL ICT to demonstrate and ensure CCG I.T network is safe and secure against Cyber-attacks.

5.   MONITORING COMPLIANCE

- The IG team will undertake ad hoc CCG IG spot checks
- The IG team will audit the shared drive and ensure named IAO for each shared high level folders are established
- The IG team will work closely with Learning and Development Team to ensure online IG training figures meet the IG toolkit requirements.

6.   EDUCATION

All staff will undertake annual online IG training via the Health E Learning Website

The IG team can deliver face to face or classroom style training to support staff if required.

The IG team will deliver IAO/IAA training as required.

The IG team will deliver training in relation to GDPR requirements

7   ASSOCIATED DOCUMENTATION

Information Governance Policy

Information Security Policy

Risk Management Framework

Serious Incident Reporting Policy

Information Governance Management Framework

Freedom of Information Policy

Health and Social Care Act 2012

Data Protection Act 1998

General Data Protection Act (May 2018 to be known as DPA 2018)

Freedom of Information/Environmental Act 2005