NHS
Wandsworth
Clinical Commissioning Group

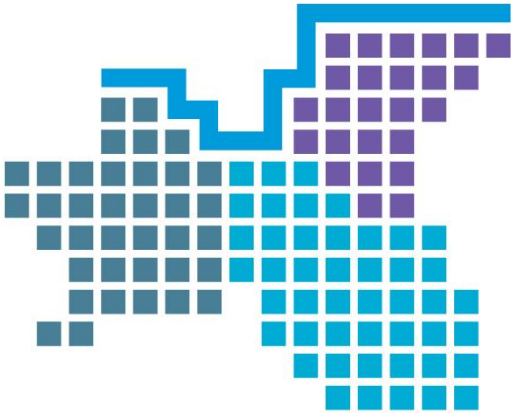
Corporate Information Security Policy

Version- Final

Date for Review: 1 December 2017

Lead Director: Performance, Quality and Cooperate Affairs

NOTE: This is a CONTROLLED Document. Any documents appearing in paper form are not controlled and should be checked against the server file version prior to use.



DOCUMENT CONTROL AND AMENDMENT RECORD

Document Name:	Corporate Information Security Policy
Consultation:	SIRO &IGSG and IGC
Approved by:	IGSG & Integrated Governance Committee(IGC)
Description:	This policy is intended to inform all staff of their responsibilities, and protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction
Audience:	All Staff
Contact details:	IG Manager
Supersedes	Information Security Policy 2012-2014

Change History

Version	Date	Author	Approver	Reason
0.1	Oct-14	IG manager		Initial Draft
0.2	Oct-14	SIRO		Review
0.3	Nov 2014	IG manager	IGSG	Approval
0.4	Dec-14	IG manager	IGC	Approval

CONTENTS

1. Introduction

The purpose of WCCG's corporate Information Security policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology and more crucially; it encompasses the behavior of the people who manage information in the line of WCCG business.

Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the WCCG is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff when working on WCCG business.
- A strengthened position in the event of any legal action that may be taken against the WCCG (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

The aim of the WCCG's Information Security Policy is to preserve:

Confidentiality	Access to Data shall be confined to those with appropriate authority
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time when it is needed.

2. Duties and Responsibilities

2.1 Chief Officer

The Chief Officer as the Accountable Officer has overall accountability and responsibility for information security, but on a day-to-day basis, the Information Governance Manager shall act as a focal point for monitoring the implementation and enforcement information security and discussion of risk issues affecting information security in WCCG. The Information Governance Manager will report directly to the Senior Information Risk Owner.

2.2 Senior Information Risk Owner

The Director of Corporate Affairs Quality and Performance/SIRO will take ownership of WCCG's information risk management policy, acts as advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of the Statement on Internal Control in regard to information risk.

2.3 Information Asset Owners

Information Asset Owners (IAO) will act as nominated owner of one or more information assets of WCCG. Their responsibilities will also include:

- Identify Information Asset Administrators to assist them with their duties, where this is appropriate and necessary.
- Document, understand and monitor what information assets are held, and for what purpose, how information is created, amended or added to, who has access to the information and why.
- Identify information necessary in order to respond to incidents or recover from a disaster affecting the information asset.
- Take ownership via input to WCCG's Information Asset Register of their local asset control, risk assessment and management processes for the information assets they own, including the identification, review and prioritisation of perceived risk and oversight of actions agreed to mitigate those risks.
- Provide support to WCCG Senior Information Risk Owner to maintain their awareness of the risks to all information assets that are owned by WCCG, for the purpose overall risk reporting requirements and procedures.
- Ensure that relevant staff are aware of and comply with expected Information Governance working practices for the effective use of owned information assets.

2.4 Information Asset Administrators

Where Information Asset Administrators (IAAs) have been identified they will;

- Ensure that policies and procedures are followed;
- Consult their information asset owners on incident management;
- The IAOs will assist the IAAs in the day to day management of information assets, identifying and reporting any information risks as and when they arise.

2.5 Line Managers

Line Managers will take responsibility for ensuring that their permanent, temporary and contractor staff are aware of:-

- Information security policies applicable in their work areas.
- Personal responsibilities for information security.
- How to access advice on information security matters.

Line managers are individually responsible for the security of their physical environments where information is processed or stored.

2.6 Staff

All staff are required to comply with information security procedures including the maintenance of data confidentiality and data integrity. Each member of staff is responsible for the operational security of the information systems they use. Failure to do so may result in disciplinary action.

3. Policy Framework

3.1 Contracts of Employment

Security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause for permanent and temporary staff. Information security expectations of staff shall be included within appropriate job definitions.

3.2 Security Control of Assets

SE CSU (Formerly SLCSU) as our ICT provider will establish an ICT asset management process and associated system, this will involve support and collaboration from the Open Service vendor where applicable. CCG will do the same for the assets managed directly by CCG

All ICT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) and information asset administrator (IAA) if required who shall be responsible for the information security of that asset.

3.3 Information Risk Assessment

All information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risks assessments are performed at least annually, following guidance form the Senior Information Risk Owner (SIRO). This should be increased to quarterly for all 'major' assets. IAO's shall submit the risk assessment results and associated mitigation plans to the SIRO for review.

3.4 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be; identified, registered and physically protected from threats and environmental hazards.

3.5 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems

and processes with third party vendors working for and on behalf of WCCG.

3.6 Information Security Events and Weaknesses management

All WCCG information security events and suspected weaknesses are to be reported to the IG Manger manager and information security officer or designated deputy and where appropriate reported as an Adverse Incident. Please see the information incident reporting in Serious Incident policy.

3.7 Classification of Sensitive Information

WCCG shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their information assets. Further details of the classifications controls can be found in the Information Life Cycle Management Policy.

3.8 Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. WCCG will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

3.9 Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a System Level Security Policy (SLSP) and are approved by the Information Security Officer and/or Corporate IT Senior Manager /IG manager before they commence operation.

3.10 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Corporate IT Senior Manager and the Information Security Officer.

3.11 Business Continuity and Disaster Recovery Plans

The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301 – Societal Security – Business Continuity Management Systems).

Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

As part of the assurance that will be provided by the CSU, The CSU will ensure that business impact assessment, business continuity, and disaster recovery plans are produced for all mission critical information, applications, systems, and networks.

3.12 Training

Information Governance training is mandatory and all staff are required to complete annual on-line Information Governance training.

3.13 Physical Security

The physical environment must be recognised as providing a layer of protection to data and information. This will be achieved by the following means:

- Controlling access to sites, buildings and offices.
- Ensuring desks and work areas are clear at the end of each day.
- Use of locked cabinets within offices to restrict access to information.
- Checking that visitors to sites are authorised to be there.
- Ensuring that when information is carried off site, it is held securely in a locked case.
- Always wearing your ID badge when on WCCG site.

3.14 Mobile Devices

- All portable media such as laptops, tablets, iphones, blackberry etc. must be encrypted and kept in secure.
- Removable media used to process CCG data must be encrypted and must not be the only source of the information (i.e. the information must also be stored in a secure folder on the Shared Drive). Such media must be kept in secure storage.

- Where staff use their own removable media , no CCG data should be stored on your personal devices e.g. if you use your own laptop, PC at home. All documents should be saved on CCG provided storage such as the shared drive via Citrix, on a CCG issued encrypted USB stick, or on the ONE drive and team sites via office 365. See Agile working policy for detailed guidance on information security and confidentiality in relation to remote/mobile working and devices.

3.15 Viruses and Malware

SECSU (formerly SLCSU) is responsible for providing IT services for WCCG, and shall implement software countermeasures and management procedures to protect WCCG against the effects of malicious software. Users shall not install software on the organisation's property without permission from the Corporate ICT Senior Manager from CSU, Information Security Officer or IG manager. Users breaching this requirement may be subject to disciplinary action.

3.16 Use and Installation of Software

- Computing equipment must not be procured or connected to any WCCG's network without the agreement of the IT service manager.
- The CSU shall ensure that security issues must be considered and documented during the requirements phase and the procurement phase of all system procurements and developments. Minimum security standards must be incorporated in all new systems.
- The CSU shall ensure that system test and live data are separated and adequately protected. All changes to the system must pass through a formal change control procedure.

3.17 Access Controls

Only authorised personnel who have a justified and approved business need must be given access to restricted areas containing information systems or stored data.

User Access Controls information will be restricted to authorised users who have a bona-fide business need to access the information.

Computer Access Control facilities will be restricted to authorised users who have a business need to use the facilities.

Application Access Control to data, system utilities, and program source libraries will be controlled and restricted to authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application will be dependent upon the availability of a licence from the supplier.

3.18 Network and Infrastructure

All network management controls and procedures will conform to the NHS wide Network Security Policy code of connection and associated guidance available from the NHS Connecting for Health website http://www.connectingforhealth.nhs.uk/

3.19 Data and Information Backup

SECSU (formerly SLCSU) will ensure that data located upon network servers will be backed in accordance with the written network back-up procedure. Such information to be stored off-site as required to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.

WCCG staff must ensure that sensitive information is not stored on individual drives, in “My Documents”, on the desktop or in email accounts in order to ensure business continuity in the event of individual unavailability. Sensitive information must be stored on the shared drive only, with restricted access or sent via nhs.net.