CORPORATE INFORMATION SECURITY POLICY:

Document History

Document Reference:	IG09
Version:	Revised Policy
Ratified by:	SL/SWL CCG SENIOR LEADERSHIP TEAMS
Date ratified	March 2018
Name of originator/author	Information Governance Services, OPTUM CSS
Name of responsible committee/individual:	Senior Leadership Team
Date issued:	March 2018
Review Date:	February 2021
Target audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to none executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Distributed via:	Website
Document Purpose:	This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations' information is maintained.

Version control sheet

Version	Section/Para/Appendix	Version/Description of Amendments	Date	Author/	Version
Revised Version Serving SL and SWL CCGs (dual branding)	Policy Review	Incorporates specific reference to impending General Data Protection Regulation (Revised as a dual branded policy for NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG) Replaces existing policies within SL and SWL CCG referenced IG09.	27/02/2018	JE	1

ASSISTANCE WITH THE APPLICATION OF THIS POLICY AND UPDATES

This policy has been prepared so as to reflect the law as at 14 February 2018. The policy will require periodic review to reflect subsequent changes to the law. Under the General Data Protection Regulation (GDPR) (which will apply from 28th May 2018), personal data must be processed in accordance with certain principles. While these are broadly similar to those under the Data Protection Directive (DPD), the wording has changed and they all centre around the concept of accountability.

The GDPR applies to 'controllers' and 'processors'; A controller determines the purposes and means of processing personal data whilst a processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The General Data Protection Regulations (GDPR) (Regulation (EU) 2016/679) – is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. GDPR applies to those who have a day to day responsibility for data protection. This should be read in conjunction with the CCGs' Information Governance Staff Handbook.

Contents

1. Introduction and Aims

Information is an asset that all staff in the NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG have a duty and responsibility to protect. The availability of complete and accurate information is essential to the CCG functioning in an efficient manner.

The CCG Corporate Information Security Policy sets out a framework for the protection of the organisation's information assets and to:

- Protect against threats, whether internal or external, deliberate or accidental
- Enable legitimate information sharing in a secure and consistent manner
- Encourage consistent and secure use of information
- Ensure that all users of CCG information have a clear understanding of their roles and responsibilities in the protection and use of information
- Ensure the continuity of IT Services and minimise disruption to business operations
- Ensure that the CCG meets its legal responsibilities

2. Scope

This policy applies to all employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff and volunteers) of the CCG. Third Parties with whom the CCG may agree information sharing protocols will be governed by the associated information sharing agreements and will be made aware of this policy. Those members of staff that are directly or indirectly employed by the CCG and for whom the CCG has legal responsibility.

This policy covers all information systems purchased, developed and managed by or on behalf of the CCG and its partners. It also applies to any person directly employed, contracted or volunteering to the CCG, all third parties and others authorised to undertake work on behalf of the CCG.

The Corporate Information Security Policy, standards, procedures and processes applies to all forms of information, including but not limited to:

- Verbal communication by telephone and social media
- Hard copy information (printed or written)
- Information stored in manual systems
- Communications, including those sent by post, courier, electronic mail, text messaging and Bluetooth
- Information that is stored in and/or processed by information systems including servers, personal computers (PC's), laptops, mobile phones, tablet devices, personal digital assistant (PDA) and any other mobile device that is allowed access to CCG information systems and information

- Information that is stored, copied, moved or transferred to any type of removable or portable media such as, but not limited to, CD's, DVD's, tapes, all types of USB devices, memory sticks
- Transmission of or passing information to third parties or others that are external to the CCG

3. Principles

3.1 Risks

- The CCG will undertake risk assessments to identify, quantify and prioritise information security risks
- Controls will be implemented to mitigate the risks identified

3.2 Organisation of Information Security

- The CCG will implement technical and operational standard policies, processes and procedures that align with ISO 27001 standards for Information Security Management
- Business continuity plans will be developed, implemented , maintained and periodically tested
- All breaches of information security, actual or suspected, will be reported and investigated

3.3 Information Security Responsibilities

- The Senior Information Risk Owner (SIRO) is the designated owner of the Corporate Information Security Policy
- Maintenance of the policy is designated to the CCG Information Governance Lead who will be supported by Information Governance (IG) expertise from the CCG's Commissioning Support Unit (contacts: lynne.wray1@nhs.net and jemptage@nhs.net)
- Line Managers are responsible for ensuring that all staff, contracted third parties etc., are made aware of and comply with the Corporate Information Security Policy including supporting policies, standards, processes and procedures

3.4 Asset Management

- All CCG assets will be accounted for and have an owner
- The CCG will implement controls that will ensure assets are appropriately protected
- Owners of such assets will be responsible for the maintenance and protection of assets they are assigned

3.5 Physical and Environmental Security

- Restricted information will be physically protected from unauthorised access, damage, interference and/or alteration
- Information processing facilities will be housed in secure areas. These areas must be protected by defined and approved security perimeters with appropriate security barriers and entry controls

3.6 Access Control

- Access to CCG information and systems will be controlled in line with appropriate System Level Security Policies etc.
- Staff will be granted access to CCG information systems and information based on their role and to a level that will enable them to carry out their employment responsibilities

3.7 Information Systems, Acquisition, Development and Maintenance

- The CCG will ensure that it commissions systems that meets the business needs of the organisation whilst at the same time recognising its dependencies on the IT Services provided by GEMCSU
- Information security requirements will be defined and communicated during the development of business requirements for new systems or changes to existing systems.
- Controls to mitigate risks identified during design, procurement, development, testing and deployment will be implemented

3.8 Information Security Incident Management

- All incidents will be managed in line with the agreed CCG Incident Reporting Policy

4. Monitoring and Review

This Policy will be reviewed at least annually and in accordance with the following as and when required:

- Legislative changes
- Good practice guidance
- Significant Incidents reported
- New vulnerabilities
- Changes to organisational infrastructure

5. Equality and Diversity Impact Assessment

The CCG aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a

disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2014 and the Human Rights Act 1998 and promotes equal opportunities for all. services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the CCG legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/ belief.

The Equality Impact Assessment has been completed and has identified impact or potential impact as “no impact”.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

6. Monitoring and Review Due Regard

Performance against Key Performance Indicators (primarily the Information Governance Toolkit) will be reviewed on an annual basis and used to inform the development of future procedural documents.

This Policy will be reviewed at least annually and in accordance with the following as and when required:

This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation, to advance equality of opportunity and foster good relations.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

Corporate Information Security Policy

Brief description of the proposal:

To ensure that the policy amends are fit for purpose, that the policy is legally compliant, complies with legislative requirements and includes details of the European Directive – General Data Protection Regulations.

Name(s) and role(s) of staff completing this assessment:

June Emptage – Information Governance Officer

Date of assessment: 27 February 2018

proposed change:

Will it affect employees, customers, and/or the public? Please

state which.

Yes it will affect all employees and those who enter into contractual arrangements with the organisation.

Is it a major change affecting how a service or policy is delivered or accessed?

No – although it introduces new General Data Protection Regulations which will be mandatory in May 2018

Will it have an effect on how other organisations operate in terms of equality?

No

If you conclude that there will not be a detrimental impact on any equality group, caused by the proposed change, please state how you have reached that conclusion:

No anticipated detrimental impact on any equality group. The policy adheres to the legislative requirements which are applicable to all.