IT ACCEPTABLE USE POLICY:

Document History

Document Reference:	IG13
Version:	Revised Policy
Ratified by:	SL/SWL CCG Senior Leadership Teams
Date ratified	March 2018
Name of originator/author	Information Governance Services
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.

South Lincolnshire CCG
South West Lincolnshire CCG

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 IG13.	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

The purpose of this document is to provide guidance to all NHS South Lincolnshire CCG and NHS South West Lincolnshire CCG Clinical Commissioning Group (CCG) staff on the acceptable use of the CCG's information or information systems and set out staff responsibility with regard to the use of information and information systems.

The aims of this document are to ensure that:

- Users are aware of their responsibilities when using CCG information and information systems
- CCG legal and statutory requirements are met
- risk of inadvertent, accidental or deliberate unauthorised access or disclosure of information is minimised
- Access to the CCG's information or information systems is controlled through a formal registration process

2. Scope

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. This policy applies to all third parties and others authorised to undertake work on behalf of the CCG. This policy applies to all who use CCG owned information technology equipment and telecommunications networks.

3. Principles

All data and information residing on the CCG information systems remains the property of the CCG at all times, unless otherwise stated.

Users accept that personal use of the CCG information systems is not a right and must be exercised with discretion and moderation. Users further accept the CCG will not accept any liability, in part of whole, for any liability for claims arising out of personal use of the CCG information systems or information.

The CCG retains the right to:

- Monitor the use of its information systems for the purpose of protecting its legitimate concerns
- Prohibit personal use of information systems where evidence points to a risk to the CCG or individually where evidence points to a breach of this or any other CCG policy
- Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not been given explicit access or authorisation
- Users are not permitted to share their, or others, usernames or passwords to gain access to CCG information systems and/or information to which they have not been given explicit authorised access
- Users must follow established procedures for password changes and are not permitted to disclose or write down their passwords

- Users are strictly prohibited from installing software on their CCG supplied device
- It is mandatory for all users to lock their terminals, workstations, laptops, by pressing ctrl/alt/del, and to ensure similar processes with iPads and/or Smartphones when not using the device
- Illegally downloading, copying and/or storage of copyrighted content onto the CCG information systems is strictly prohibited.
- All users must follow the CCG Health and Safety guidelines when using CCG information systems
- Users are strictly prohibited from using CCG information systems and information in a manner that will:
- Break the law and/or have legal implications or liability to the CCG
- Cause damage or disruption to CCG information systems
- Violate any provision set out in this or any other policy

Usage of the CCG internet is primarily for business use. Occasional and reasonable personal use is permitted, e.g. during lunch breaks, provided that such use does not interfere with performance of duties and does not conflict with CCG policies, procedures and contracts of employment.

Users must, at all times, comply with Copyright, Design and Patent Laws, when downloading material from internet sites.

The CCG prohibits access to websites deemed inappropriate and monitors access and usage. The monitoring information may be used to support disciplinary action.
Sites deemed inappropriate are those with material that is:

- Defamatory, pornographic, sexist, racist, or about on-line gambling, terrorism and/or such sites whose publication are illegal or risks causing offence.

Users must not circumvent, cause to circumvent or use tools to circumvent prohibited website controls. If a user inadvertently accesses an inappropriate website, the user must immediately inform their line manager or the IT Service Desk.

Financial transactions are not permitted on websites requiring software to be downloaded prior to the transaction being executed. The CCG accepts no responsibility for any charges and/or losses incurred in relation to personal purchases or personal transactions using the CCG information systems regardless of cause.

4. Accountability

Overall responsibility for the Acceptable Use policy lies with the Senior Information Risk Owner (SIRO) of the CCG who has delegated responsibility for managing the development and implementation of procedural documents to the Information Governance Lead in the CCG. Support is provided from the Optum Commissioning Support Services Information Governance Team under a Lead Provider Framework Contract. The CCG may take disciplinary action against users found to have contravened this Acceptable Use Policy.

5. Equality and Diversity

5.1 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 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

5.2 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.

5.3 In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

6. Due Regard

6.1 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

7. Policy Review

This policy will be reviewed annually in line with Information Governance Toolkit requirements or where changes occur with legislation or national policy.

Appendix 1 - Equality Analysis Initial Assessment

Title of the change proposal or policy:

IT Acceptable Use 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.