NHS
Leeds
Clinical Commissioning Group

Acceptable Use Policy

Version:	1
Ratified by:	Audit Committee
Date ratified:	16 September 2020
Name & Title of originator/author:	Abi Dakin
Name of responsible committee/individual:	Information Governance Committee
Date issued:	September 2020
Review date:	September 2022
Target audience:	All staff

Executive Summary

This policy is part of a set of Information Management and Governance policies and procedures that support the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies.

Equality Impact Assessment (EIA)

This document has been assessed, using the EIA toolkit, to ensure consideration has been given to the actual or potential impacts on staff, certain communities or population groups, appropriate action has been taken to mitigate or eliminate the negative impacts and maximise the positive impacts and that the and that the implementation plans are appropriate and proportionate.

Contents

Table of Contents

1 Introduction

This policy is part of a set of Information Management and Governance policies and procedures that support the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies.

The Acceptable Use Policy (AUP), is a set of rules applied by the CCG, as the data and equipment owners; it looks to mandate the ways in which the network and managed devices provided may be used.

All electronic equipment is provided in order to facilitate the conduct of the CCG's business and any serious misuse or misappropriation of assets could result in legal or disciplinary action.

2 Scope

This policy applies to everyone who has access to CCG data, electronic information assets, systems, applications or IT equipment. This may include, but is not limited to, all employees, non-executive director, consultants, contractors and agents employed by the CCG and partner organisations who are provided with authorised access to the CCG data storage and data processing equipment, systems or data. These people are referred to as 'users' in this policy.

All those who use or have access to CCG information must understand and adopt this policy and are responsible for ensuring the security of the CCG's information systems and the information that they use or handle.

This policy covers all Information Systems (IS) environments operated by Leeds CCG or contracted with a third party for use by Leeds CCG. .

3 Personal Responsibility

Devices are issued for work purposes and remain the property of the CCG. Users are responsible for the safety and use of the equipment throughout the duration of their work with Leeds CCG.

3.1 Changing Role or Team

Users and their managers MUST comply with the instructions provided in the Starters, Movers and Leavers guidance if they move from one area of the CCG to another.

3.2 Leaving the CCG

Users MUST return all their CCG equipment directly to their manager when they leave the CCG.

Detailed information in the form of a checklist about making necessary arrangements for the return of equipment are provided in the Starters, Movers and Leavers guidance.

4 Personal Use

4.1 Users are allowed to utilise their CCG devices and the CCG network for personal, non-pornographic, legal use within reason outside office hours, or during breaks.

4.2 Due to the nature of CCG business and the personal data it protects, users MUST NOT allow anyone else, including family members to use the device **unless supervised**.

4.3 Activities undertaken by others shall be deemed attributable to the user logged in at the time.

4.4 Users should be aware that any data stored on the device provided or the CCG network may be subject to scanning and monitoring in the future to ensure the protection of the wider environment.

4.5 For offers available to NHS staff, it is acceptable to sign up to non-work-related web-accounts where a NHSmail.net email address is required, however, there must not be any re-use of NHSmail passwords.

4.6 Users MUST NOT sign up to accounts using their work mobile account which will bill to the CCG nor must they use CCG data for personal use.

4.7 Users MUST NOT reuse a CCG Network Login ID and/or password.

There are no instances when accessing an individual's data for personal use is acceptable. Personal information should only be accessed in relation to your work remit

5 Monitoring

For the purposes of this document, monitoring refers to the protective analysis of activities undertaken by users and systems.

5.1 Users must be aware that the CCG may monitor and control access to CCG information assets and the internet.

5.2 Blanket monitoring of the CCGs' systems and networks may occur systematically in the background of daily processing.

5.3 Monitoring for illegal activity may occur in much the same way. However, should a user's account be discovered to be engaged in illegal activities or activities as described in the disciplinary policy this may result in prosecution and/or disciplinary action.

5.4 If an incident occurs, the CCG may utilise audit functionality to retrospectively audit access and activities undertaken on CCG systems and devices

6 Scanning

For the purposes of this document scanning refers to an automated activity that inspects data for malicious file types or illegal activity.

6.1 Users should be aware that the CCG scans the end-user-devices, the CCG network and any removable media connected to CCG devices, including USB sticks, hard drives, cameras, mobile phones etc.

6.2 Malicious file types may be detected at the boundary of the network at internet and email gateways; these will be prevented from entering where possible.

6.3 Malicious file-types can be detected from removable media, USB sticks, hard drives, CDs etc and are scanned when connected to the estate e.g. your computer.

7 Personal Devices and Data

7.1 If you connect your own, personal device to your CCG provided device or the CCG network, the data on your personal device may be scanned for illegal activity.

7.2 If you transfer any of your own, personal data, including photographs and videos to the CCG network, it will be subject to the same scanning protocol as described in section 6.

8 Use of Email and instant Messenger

8.1 Acceptable Use https://portal.nhs.net/Home/AcceptablePolicy

8.1.1 Please consider your actions in line with the Disciplinary & Behaviour Policies.

8.1.2 Users MUST maintain a professional tone in all communications.

8.1.3 Email is a messaging tool, any records received into email MUST be stored appropriately and have the CCG's retention schedule applied.

8.1.4 Users MUST consider the audience of each communication. Users must consider whether is it appropriate to 'reply all' in all circumstances.

8.2 Unacceptable Use

8.2.1 Users MUST NOT expand the circulation of an email trail without considering the nature of content or the senders' instructions

8.2.2Users MUST NOT send content that is illegal or breaches the Disciplinary & Behaviour Policies

8.2.3 Users MUST NOT breach confidentiality or commercial in Confidence rules.

9 Social Media

Users should seek support if they feel they are being targeted on social media for work they do on behalf of the CCG.

9.1 Acceptable Use

9.1.1 Users MAY use their CCG device to access their personal social media accounts. Please update privacy setting in order to protect yourself from unwanted contact.

9.1.2 Employees working directly with service users MUST take action to reduce inappropriate contact by using the appropriate privacy settings.

9.2 Unacceptable Use

9.2.1 Users MUST NOT express or share negative opinions about work, CCG staff or services on social media.

9.2.2 Users MUST NOT, express opinions that breach the Disciplinary & Behaviour Policies on social media.

10 Network Drives, Fileshare and Removable Media

10.1 Acceptable Use

10.1.1 When changing role, users MUST NOT access files made accessible by a previous role, except where such access remains relevant.

10.1.2 The L: drive MUST be used as the 'service shared area'. This space is intended to help you store and share files with other staff in the same service.

10.1.3 The F: drive is a secure storage space which only you can access. Files that contain your personal information COULD be saved here.

10.1.4 The C: drive is considered as the primary hard drive of the system and is used for storing the operating system, system files and other applications and their related files.

10.2 Unacceptable Use

10.2.1 Users MUST NOT save personal, special category or confidential information in the L: drive unless it is saved to a secure folder with secure access controls in place

10.2.2 Users SHOULD NOT save documents to the C:\ drive as normal practise, as it is not backed up and information may be lost or deleted if you experience any issues with your computer. This includes your desktop and in some cases 'My Documents'. The C:\ should only be used to save records where there is no alterative or storage is only for a short temporary period. Any files created on C:\ should be transferred into the relevant place on the network drive at the earliest opportunity.

10.2.3 Users MUST NOT use the corporate file shares to store personal photographs, videos, downloadable content, or other copyrighted material, e.g. films or TV Boxsets.

10.2.4 Users MUST NOT transfer CCG data to removable media.

10 Compliance

If you fail to comply with this policy you may be referred to the formal policy, including the Disciplinary Policy and Procedure. Depending on the circumstances, including the seriousness of any breach of the Disciplinary & Acceptable Standards and Behaviours Policies, a potential outcome of disciplinary action could result in your dismissal with or without notice or payment in lieu of notice.

11 Associated Documents

Information Security Policy
Confidentiality and Data Protection Policy
Email Policy
Information Governance Policy and Management Framework
Internet and social Media Policy
Acceptable Standards and Behaviours Policy
Disciplinary Policy

Title of document	Acceptable Use Policy
Author	Abi Dakin
New / Revised document	New
Lists of persons involved in developing the policy List of persons involved in the consultation process:	Abi Dakin Carrick Armer Ian Corbishley Karen Rowe Information Governance Committee Members