Approved Sept 2020

NHS
North West London
Collaboration of
Clinical Commissioning Groups

IT Acceptable Use Policy

Version 1.2

V1.3 September 2020

Version Control

Version Number	Reviewing Committee / Officer	Date
1.0	NHS NW London Clinical Commissioning Group, IT Security & Cyber Security Team	07/03/19
1.1	Access to Remote Desktop services added to section 3.4	18/06/2020
1.2	Accepted amendments by NWL DPO	29/06/2020
1.3	Updates by SIRO	21/09/20

Reviewers

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Abhilash Abraham		Head of IT & Cyber Security	19 Jun 2020	1.2
Ernest Norman-Williams		NWL General Practice Data Protection Officer	26 June 2020	1.2
Felicia AYO-AJALA		NWL Data Protection Officer	26 June 2020	1.2
Victoria Medhurst		Senior Information Risk Owner	28/8/20	1.2
Jenny Greenshields		SIRO	21/09/20	1.3

Approvals

This document must be approved by the following:

Title	Signature	Title / Responsibility	Date	Version
NWL CCGs Governing Bodies	--------------	NWL CCGs Governing Bodies	Sept 2020	1.3

NHS
North West London
Collaboration of
Clinical Commissioning Groups

Contents

1. Introduction 4

1.1 The Information Security Management System (ISMS) 4

2. Purpose 4

3. Computer Conditions of Use 4

3.1 Introduction & Policy 4

3.2 NWL CCG Computer Systems Conditions of Use Policy 5

3.3 Equipment 6

3.4 Connecting remotely and home users 6

3.5 Identities and Passwords 7

3.6 Offensive and Inappropriate Material 8

3.7 Physical Security 8

4. Additional User Policies and Guidance 8

Appendix 1 12

Equality Impact Assessment Tool (Equality Analysis) 12

1. Introduction

This document forms part of the NHS North West London Collaboration of Clinical Commissioning Group (NWL CCG) Information Security Management System.

It provides statements detailing acceptable use whilst accessing and using NWL CCG IT Services & Systems.

1.1 The Information Security Management System (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards and architectures that: -

- Set out the governance of IT security;
- Provide high level policy statements on the requirements for managing IT security;
- Define the roles and responsibilities for implementing the IT security policy;
- Identify key standards, processes and procedures to support the policy;
- Define security architectures that encapsulate the policy and support the delivery of secure IT services.

2. Purpose

This document provides the detailed policy statements for the acceptable use of IT services.

3. Computer Conditions of Use

3.1 Introduction & Policy

NWL CCGs believe it is important to encourage the use of E-mail, internet, and its computer systems for the benefit of the NHS community. At the same time, NWL CCGs need to protect their interests and those of its employees. In order to achieve this balance, the conditions of use are defined, and all users must comply.

The purpose of the Acceptable Use Policy (AUP) is to ensure that users of the NWL CCG computer systems do so in a secure, lawful and responsible manner.

The conditions of use, along with acceptable use standards, policies and supporting guidelines listed here, are reviewed annually.

All NWL CCG employees, as well as any contractor, consultant or employee of a partner organisation, who are provided with access to any computer service provided by NWL CCG must comply with these statements. Failure to do so could lead to access to the computer systems being withdrawn and, in the case of employees, disciplinary action taken.

Staff should speak to your line manager if you require further advice on any aspect of complying with these statements.

3.2 NWL CCG Computer Systems Conditions of Use Policy

All users of NWL CCG computer systems, as a condition of use, are required to

- Comply with the acceptable use standards, GDPR, Data Protection and Computer Misuse Acts;
- Be aware of, and comply with NWL CCG Information security policies;
- Be aware that usage monitoring and reporting may be undertaken;
- Be individually responsible for maintaining security.

Accessing the Internet and Using E-mail
NWL CCG systems may be used for limited personal use at the discretion of your manager **provided that this never:**

- interferes with NWL CCG work;
- relates to a personal business interest;
- is unlawful;
- brings NWL CCG into disrepute.

NWL CCG systems **must not** be used:

- for the creation, use, transmission or encouragement of material which is illegal, obscene, libellous (defamatory), offensive, threatening, harassing or discriminatory;
- to transmit unsolicited commercial or advertising material;

- for illegal activities including breaching the GDPR, Data Protection, Computer Misuse and Design, Copyright and Patents Acts;
- for violating or otherwise intruding upon other people's privacy;
- to wilfully disrupt other users' work in anyway, including with viruses or by corrupting data;
- to express personal views which could be misinterpreted as those of NWL CCG or which are prejudicial to the interests of the organisation;
- to commit the organisation to purchasing or acquiring goods or services without proper authorisation

Use of Social Media and Social Networking

Social networking sites (e.g. Facebook, Twitter) are public forums so therefore must not be used for the discussion of NWL CCG/NHS related business and/or activities, unless authorised or from a corporate account (e.g. Media / Communication team).

Supporting Guidance

NWL CCG users are encouraged to identify all personal E-mails by typing 'personal/private' in the E-mail subject line, and file into a separate folder, against which regular housekeeping is performed.

3.3 Equipment

Computers must be locked manually (CTRL-ALT-DEL-Enter, Windows Key+L) when leaving a workstation unattended.

Users must not connect an office based workstation to an external network such as the Internet (for example via an open non-approved wifi connection) at the same time as it is connected to an internal NWL CCG network, unless approved by senior management and protected by additional security controls (such as use of a "personal firewall") that have been agreed with IT Services in advance.

All NWL CCG supplied IT Services equipment and any data created using the organisations systems remains at all times the property of NWL CCG.

NWL CCG IT equipment must be returned (and/or destroyed as advised) on termination of employment or business relationship with NWL CCG or upon request.

Any Information that needs to be shared with other NWL CCG staff must only be shared using the NWL CCG provided shared network folders and/or NWL CCG provided collaborative working tools.

Local file sharing is not permitted.

3.4 Connecting remotely and home users

Where users are provided with access from, or computers for use at home, it is the user's responsibility to ensure that no unauthorised or inappropriate use (as defined in this policy) is made of that computer.

Only remote access solutions that are provided or agreed with NWL CCG can be used to access NWL CCG networks when away from NWL CCG workplaces.

Workstations which have remote access to NWL CCG internal networks via the Internet must be protected from intrusion (for example, by setting passwords and using the latest versions of anti-virus software) to prevent unauthorised access to the NWL CCG networks and systems. (NWL CCG IT support will provide advice and may supply approved solutions for use in such situations).

RDP access to desktops is only allowed by special request and agreement with NWL CCG and only permitted from remote clients running on equipment provided by NWL CCG. RDP from a remote client running on a private device is not permitted.

Where users have obtained prior authorisation to use third party remote access tokens to access the network, the user or practice agrees to assist NWL CCG in any security/cyber breach investigation which might also include providing permission for the third party provider to release audit logs of their token usage to NWL CCG.

3.5 Identities and Passwords

An individual identity will be allocated to you. This means that you are accountable for all actions performed under that identity.
Your password and, if provided, security token, are the keys to preventing others from misusing your identity.

- All users will be allocated a unique user identity for the systems that they are permitted to use;
- You must not allow others to use systems under your identity;
- You are accountable for all actions performed under your identity.

Where you have reason to believe that your password has been disclosed to others, you must change it immediately and you must report this as a potential security incident with the IT service desk.

Information

Sensitive information (defined as information which is personally identifiable and or commercially confidential) must not be stored on workstations local disks or mobile devices unless there is a business requirement, with a formal risk assessment undertaken prior to approval. It will be necessary to protect the information by an approved file or disk encryption mechanism.

Supporting Guidance: Tasks which access sensitive information should not be performed on workstations in public areas. Consult your manager for guidance. Where business requirements dictate that this is essential, the screen should be positioned to ensure that the sensitive information cannot be overlooked.

3.6 Offensive and Inappropriate Material

The use of NWL CCG supplied equipment to access, store, copy or distribute items which are inappropriate, offensive, libellous (or in some other way illegal) or may jeopardise security in any way is prohibited. Users should be aware that to do so could constitute a prosecutable offence under UK law.

3.7 Physical Security

Handheld devices should be kept in your possession or locked away when not in use. Equipment should not be left in cars. Where unavoidable, it must be locked, out of sight either in the boot or a locked glove compartment.
Users must ensure that NWL CCG supplied workstations are installed in a physically secure part of the building to protect them from theft and inappropriate or unauthorised use.

4. Additional User Policies and Guidance

E-mail and Internet Monitoring Policy

To protect its interests and ensure compliance with regulatory or self-regulatory policies and guidelines, NWL CCG reserves the right to monitor the use of E-mail and the Internet and, where necessary, data will be accessed or intercepted. A data protection impact assessment will be carried out before such monitoring occurs. Staff will be made aware with associated reasons why the monitoring should take place

Incident Reporting Guide

For the protection of NWL CCG information and IT infrastructure and services, all employees and contractors have a duty to report all potential security incidents as soon as possible when they are discovered via the following:

- **your line manager**, by phone, E-mail or in person;
- **NWL Service Desk; nwlccg.servicedesk@nhs.net**
- **the IT & Cyber Security Team nwlccgs.security@nhs.net**

The following types of incidents must be reported:

- Any suspected misuse of NWL CCG computer systems, whether accidental or deliberate;
- A system or network security control that is (or is in danger of being) disabled or ineffective;
- A virus or worm infection is suspected on a laptop, workstation or server – note you must immediately turn the device off and then report it;
- Where you discover or suspect user behaviour which does not comply with the computer condition of use or any other information security policies;
- Where you suspect that sensitive information is being disclosed or modified without proper authority.

Information received by line, section or corporate managers regarding suspected or actual breaches of security will be treated confidentially.

Legal Compliance Guide

All users of NWL CCG computer systems should be familiar with the key provisions of the following legislation:

- Data Protection Act 2018;
- General Data Protection Regulation (GDPR 2016)
- Copyright, Designs and Patents Act 1998;
- Human Rights Act 1998;
- Computer Misuse Act 1990;
- Regulation of Investigatory Powers Act 2000;
- Criminal Justice and Immigration Act 2008.

In addition users should be aware of the following related points.

Electronic mail

Like all correspondence, E-mail cannot be regarded as purely private and only seen by the intended recipient. It may also be regarded as official correspondence of NWL CCG.

Remember that E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. Therefore be aware that:

- **E-mail has been used successfully as evidence in libel cases and industrial tribunals. Sending defamatory mail, even internally, could make NWL CCG liable to pay heavy damages to injured parties.**

It should also be noted that the GDPR/Data Protection Act 2018 gives data subjects the right to request disclosure of their personal details contained in E-mails.

Copyright

Under the Copyright, Designs & Patents Act 1998 the illegal copying of software is regarded as theft.

The rights of computer software designers/writers are protected by this Act. It is an offence to copy, publish, adapt or use computer software without the specific authority of the copyright holders.

It is also important to be aware that all software or data files developed by staff on NWL CCG computing equipment are the property of NWL CCG. They may not be made available for use outside of NWL CCG without prior approval.
Any breach of the Act could result in disciplinary or even legal action. Managers should ensure that all software has been obtained legally.

Licensing

To comply with legislation, and to ensure on-going vendor support, the terms and conditions of all licensing agreements must be adhered to. All software and other applicable materials must be appropriately licensed (if required) whether installed or used on NWL CCG or personal equipment.

As is the case in obtaining products by any other means, all licensing requirements, payment conditions and deletion dates associated with downloaded software must be met. Anyone downloading software must be aware of the difference between:

- Copyrighted Software- requires a licence payment;
- Freeware - licensed but requires no payment;
- Shareware - copyrighted but often free for a trial period;
- Public Domain Software- which is free.

Third-party information

Some of the information you receive or obtain from clients, suppliers and other third parties may be confidential or contain proprietary information. Like any other confidential information NWL CCG has a duty to maintain its confidentiality and only use it for certain limited business purposes consistent with any applicable agreements which NWL CCG may have with the third party.

When making use of third party information users should be aware that such information may be protected by intellectual property rights (e.g. copyright under the Copyright, Designs & Patents Act 1988) and such usage may be subject to limitations and restrictions. Particular care is needed when sending attached files or reproducing information from the Internet.

Appendix 1

Equality Impact Assessment Tool (Equality Analysis)

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

		Yes/ No	Comments
1	**Does the policy/guidance disadvantage one group or more than another on the basis of:**		
	• Race (including colour, culture, ethnicity, nationality or national origin and the travelling community)	N	
	• Religion or Belief	N	
	• Sex (e.g. male or female)	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation (Lesbian, Gay, Bisexual, Heterosexual)	N	
	• Gender reassignment (e.g. someone who 'is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.')	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (children, young adolescent, older people etc.)	N	
2	**Is the policy/guidance/strategy more favourably towards one group on the basis of:**		
	• Race	N	

	• Religion or Belief	N	
	• Sex	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation	N	
	• Gender reassignment	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (e.g. children, young adolescent, older people etc.)	N	
3	**If you have identified potential discrimination in the policy/guidance are there any valid, legal and/or justifiable exceptions? Please list any exceptions.**	N/A	
4	**Is the policy/guidance likely to have a negative/adverse impact on any of the above group(s)?**	N/A	
5	**If so, how would you address the impact? Please explain.**	N/A	
6	**What are the associated objectives to the policy/guidance?**		See section 2 of policy

If you have identified a potential discriminatory impact in this document, please refer to the author(s) of the policy/guidance, together with any suggestions required to address the impact.