Acceptable Use Policy

Policy Number	
Version:	V1.0
Ratified by:	NEH&F Audit and Risk committee
Date ratified:	8th August 2017
Name of Responsible Officer/author:	Matthew Wall – SCW IG Manager
Date issued:	10th August 2017
Next Review date:	8th August 2018

Version Control:

History			
Version	Date	Author(s)	Comments
0.1	21.06.17	Matt Wall	SCW policy adopted for CCG/Partnership, addition of Analysing the Impact on Equality appendix
1.0	10.8.17	Matt Wall	Approved Policy published

Contents

1 Introduction

This document forms part of the NHS North East Hampshire and Farnham CCG Information Security Management System, which includes the partnership working arrangements of the Hampshire CCG Partnership which comprises of NHS North East Hampshire and Farnham CCG, NHS Fareham and Gosport CCG, NHS North Hampshire CCG, and NHS South Eastern Hampshire CCG)

It provides statements detailing acceptable use whilst accessing and using CCG/Partnership 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.

1.2 Document Purpose

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

2 Computer Conditions of Use

2.1 Introduction & Policy

The CCG/Partnership believes 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, the CCG/Partnership needs to protect its interests and those of its employees or clients. In order to achieve this balance, the conditions of use are defined and all users must comply.

The purpose of the Acceptable Use Policy is to ensure that users of the CCG/Partnership's 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 CCG/Partnership employees, as well as any contractor, consultant or employee of a partner organisation, who are provided with access to any computer service provided by the CCG/Partnership 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.

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

2.2 CCG/Partnership Computer Systems Conditions of Use Policy

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

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

Accessing the Internet and Using E-mail

CCG/Partnership systems may be used for limited personal use at the discretion of your manager

Provided that this never:

- interferes with CCG/Partnership's work;
- relates to a personal business interest;
- is unlawful;
- brings the CCG or partnership into disrepute.

CCG/Partnership 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 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 the CCG, the Partnership or which are prejudicial to the interests of the CCG or Partnership;
- to commit the CCG or Partnership 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 CCG/Partnership related business and/or activities, unless authorised or from a corporate account (e.g. Media / Communication team).

Supporting Guidance

CCG/Partnership 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.

2.3 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 CCG/Partnership provided network, unless approved by senior management and protected by additional security controls (such as use of a "personal firewall") that have been agreed with SCW CSU IT Services in advance.
All CCG/Partnership supplied IT Services equipment and any data created using the organisations systems remains at all times the property of CCG/Partnership.
CCG/Partnership IT equipment must be returned (and/or destroyed as advised) on termination of employment or business relationship with CCG/Partnership or upon request.
Any Information that needs to be shared with other CCG/Partnership staff must only be shared using the CCG/Partnership provided shared network folders and/or CCG/Partnership provided collaborative working tools.
Local file sharing is not permitted.

2.4 Connecting remotely and home users

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 the CCG/Partnership can be used to access CCG/Partnership networks when away from CCG/Partnership workplaces.

Workstations which have remote access to CCG/Partnership 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 CCG/Partnership networks and systems. IT service desk will provide advice and may supply approved solutions for use in such situations).

2.5 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.

2.6 Offensive and Inappropriate Material

The use of CCG/Partnership 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.

2.7 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 CCG/Partnership supplied workstations are installed in a physically secure part of the building to protect them from theft and inappropriate or unauthorised use.

3 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, the CCG/Partnership reserves the right to monitor the use of E-mail and the Internet and, where necessary, data will be accessed or intercepted.

Incident Reporting Guide

For the protection of CCG/Partnership 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;
- **SCW CSU Service Desk;**
- **SCW CSU Information Governance Manager.**

The following types of incidents must be reported:

- Any suspected misuse of CCG/Partnership 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 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 CCG/Partnership Staff computer systems should be familiar with the key provisions of the following legislation:

- Data Protection Act 1998;
- 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 CCG/Partnership. 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 the CCG/Partnership liable to pay heavy damages to injured parties.**

It should also be noted that the Data Protection Act 1998 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 supplied CCG/Partnership computing equipment are the property of the CCG and/or Partnership. They may not be made available for use outside of CCG/Partnership 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 ongoing 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 CCG/Partnership 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 the CCG/Partnership has a duty to maintain its confidentiality and only use it for certain limited business purposes consistent with any applicable agreements which the CCG/Partnership 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.

End of Policy Statement

Appendix 1

Analysing the Impact on Equality

1. Title of policy/ programme/ framework being analysed IT Services – Acceptable Use Policy V2.1
2. Please state the aims and objectives of this work and the *intended equality outcomes*. How is this proposal linked to the organisation's business plan and strategic equality objectives? To ensure and raise staff awareness of acceptable use of IT equipment and systems
3. Who is likely to be affected? e.g. staff, patients, service users, carers Staff
4. What evidence do you have of the potential impact (positive and negative)?
4.1 Disability (Consider attitudinal, physical and social barriers) no impact
4.2 Sex (Impact on men and women, potential link to carers below) no impact
4.3 Race (Consider different ethnic groups, nationalities, language barriers, cultural differences). no impact
4.4 Age (Consider across age ranges. This can include safeguarding, consent and child welfare). no impact
4.5 Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment). no impact
4.6 Sexual orientation (This will include lesbian, gay and bi-sexual, heterosexual people). no impact
4.7 Religion or belief (Consider impact on people with different religions, beliefs or no belief) no impact
4.8 Marriage and Civil Partnership no impact
4.9 Pregnancy and maternity (impact on working arrangements, infant caring responsibilities). no impact
4.10 Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation)**.** no impact
4.11 Additional significant evidence (Give details of any evidence on other groups experiencing disadvantage and barriers to access due to: socio-economic status, location (e.g. living in areas of multiple deprivation), resident status (migrants), multiple discrimination, homelessness, no impact
5 Action planning for improvement Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning. Not applicable

Sign off
Name and signature of person who carried out this analysis Matthew Wall Information Governance Manager NHS South, Central and West CSU
Date analysis completed 21st June 2017