NHS
Buckinghamshire
Clinical Commissioning Group

FINAL

Acceptable Use Policy
Version 2

Buckinghamshire CCG
March 2019

South, Central and West

DOCUMENT CONTROL

Document Name	Version	Status	Author
Acceptable Use Policy	*2.0*	*Final*	*BCCG Cyber Security Manager*
Document objectives:	*The objective of this policy is to protect the information assets owned and used by the BCCGBCCG, from all threats, whether internal or external, deliberate or accidental and to meet all regulatory and legislative requirements.* *Purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at BCCGBCCG in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.*		
Target audience:	*All staff*		
Committee/Group Consulted:	*BCCG Information Governance Steering Group*		
Monitoring arrangements and indicators:	*This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.*		
Training/resource implications:	*All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet corporate policies pages*		
Approved and ratified by:	*BCCG Information Governance Steering Group* *BCCG Exec Committee*	*Date:*	
Equality Impact Assessment:	*Yes*	*Date: 23 July 2018*	
Date issued:	*Jan 2019*		
Review date:	***January 2021***		
Author:	*Cyber Security Manager*		
Lead Director:	*Director of IT Services*		

Version Control

Date	Author	Version	Page	Reason for Change
14/12/2017	SCW CSU IT Services	1.0		Policy review date to align with GDPR after approval from SCW Information Governance Steering Group
01/01/2019	BCCG	2.0		Policy review date to align with GDPR for approval from BCCG Information Governance Steering Group

CONTENTS

1 INTRODUCTION

This document forms part of the NHS Buckinghamshire Clinical Commissioning Group Information Security Management System.

It provides statements detailing acceptable use whilst accessing and using BCCG 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 SERVICES acceptable use.

2 COMPUTER CONDITIONS OF USE

2.1 INTRODUCTION & POLICY

BCCG 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, BCCG needs to protect its 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 BCCG 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 BCCG employees, as well as any contractor, consultant or employee of a partner organisation, who are provided with access to any computer service provided by BCCG 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.

BCCG Computer Systems Conditions of Use Policy

All users of BCCG computer systems, as a condition of use, are required to:

- Ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation Act (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national laws implementing them as amended from time to time.

- In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations
- Comply with the acceptable use standards and Computer Misuse Acts
- Be aware of, and comply with BCCG 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

BCCG systems may be used for limited personal use at the discretion of your manager **provided that this never:**

- interferes with NHS Buckinghamshire CCG work
- relates to a personal business interest
- is unlawful
- brings BCCG into disrepute

BCCG 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 General Data Protection Legislation, 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 BCCG 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 BCCG/NHS related business and/or activities, unless authorised or from a corporate account (e.g. Media / Communication team).

Supporting Guidance

BCCG 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.

2.2 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 BCCG 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 BCCG supplied IT Services equipment and any data created using the organisations systems remains at all times the property of BCCG.

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

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

Local file sharing is not permitted.

2.3 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 BCCG can be used to access BCCG networks when away from BCCG workplaces.

Workstations which have remote access to BCCG 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 BCCG

networks and systems. (BCCG IT support will provide advice and may supply approved solutions for use in such situations).

2.4 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. See the *IT Services Password Policy* for detailed password policy statements.

Information

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The

	definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to BCCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

'Special Categories' of Personal Data, Personal Confidential Data or Commercially confidential Information 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 Special Categories' of Personal Data, Personal Confidential Data and Commercially Confidential 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 information cannot be overlooked.

2.5 OFFENSIVE AND INAPPROPRIATE MATERIAL

The use of BCCG 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.

2.6 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 BCCG 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

3.1 E-MAIL AND INTERNET MONITORING POLICY

To protect its interests and ensure compliance with regulatory or self-regulatory policies and guidelines, BCCG reserves the right to monitor the use of E-mail and the Internet and, where necessary, data will be accessed or intercepted.

3.2 INCIDENT REPORTING GUIDE

For the protection of BCCG 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
- **BCCG Service Desk**
- **Information Security Manager**
- **Incident management system – Datix**

The following types of incidents must be reported:

- Any suspected misuse of BCCG 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 personal and / or 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.

3.3 LEGAL COMPLIANCE GUIDE

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

- General Data Protection Regulation (EU) 2016/679 (GDPR)
- Data Protection Act (DPA) 2018
- Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time
- All applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998
- Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015
- Common law duty of confidentiality
- Privacy and Electronic Communications (EC Directive) Regulations

In addition, consideration must also be given to the

- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Records Act 1990
- Fraud Act 2006
- Bribery Act 2010
- Criminal Justice and Immigration Act 2008
- Equality Act 2010
- Terrorism Act 2006
- Malicious Communications Act 1988
- Digital Economy Act 2010 and 2017
- Counter-Terrorism and Security Act 2015

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

3.4 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 BCCG. 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 BCCG liable to pay heavy damages to injured parties**

It should also be noted that under the Right of Access under the GDPR (Article 15), an individual has the right to request disclosure of their personal details contained in E-mails.

3.5 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 BCCG computing equipment are the property of BCCG. They may not be made available for use outside of BCCG 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.

3.6 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 BCCG 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.

3.7 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 BCCG has a duty to maintain its confidentiality and only use it for certain limited business purposes consistent with any applicable agreements which BCCG 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 A - EQUALITY IMPACT ASSESSMENT

For Acceptable Use Policy

1. Title of policy/ programme/ framework being analysed Acceptable Use Policy.
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 provide a framework of guidance to NHS South, Central and West CSU (SCW) staff (as defined in the scope) regarding the security of Personal and Sensitive Data in both paper and electronic form.
3. Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers Staff.
4. What evidence do you have of the potential impact (positive and negative)? None expected.
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, Roma Gypsies, Irish Travellers, language barriers, cultural differences). No impact
4.4 Age (Consider across age ranges, on old and younger people. 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 people as well as 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 (This can include impact on working arrangements, part-time working, 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 (See Guidance Note) 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 (See Guidance Note) 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.
Sign off
Name and signature of person who carried out this analysis Beverly Carter Head of IG, NHS South, Central and West Commissioning Support Unit
Date analysis completed 23 July 2018
Name and signature of responsible Director Simon Sturgeon, IT Services Director
Date analysis was approved by responsible Director 23 July 2018

End of Policy Document