NHS
Bristol, North Somerset
and South Gloucestershire
Clinical Commissioning Group

IT Acceptable Use Policy

Shaping better health

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	48
Responsible Executive Director:	Sarah Truelove, Deputy CEO and Chief Finance Officer.
Author and Job Title:	Jane Schofield, Digital Business Partner
Date Approved:	March 2020
Approved by:	Sarah Truelove, Deputy CEO and Chief Finance Officer.
Date of next review:	March 2022

	Yes/No/NA	**Supporting information**
Has an Equality Impact Assessment Screening been completed?	Yes	
Has the review taken account of latest Guidance/Legislation?	Yes	
Has legal advice been sought?	N/A	Draft policy produced by CSU
Has HR been consulted?	N/A	
Have training issues been addressed?	Yes	Support is available via the IT helpdesk
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by JCC?	No	
Are there financial issues and have they been addressed?	No	This policy covers the use of IT equipment which is funded through existing budgets
What engagement has there been with patients/members of the public in preparing this policy?	N/A	
Are there linked policies and procedures?	Yes	This policy is one of a suite of IT?IG related documents which support the CCG's responsibilities listed in the Data Security Protection Toolkit
Has the lead Executive Director approved the policy?	Yes	
Which Committees have assured the policy?	N/A	Information Governance Group are aware of the policy which has also been reviewed by the Corporate Policy Review Group
Has an implementation plan been provided?	Yes	
How will the policy be shared with: • Staff? • Patients? • Public?		See Implementation Plan
Will an audit trail demonstrating receipt of policy by staff be		

required; how will this be done?		

Table of Contents

IT ACCEPTABLE USE POLICY

SUMMARY OF KEY POINTS TO NOTE

The purpose of this policy is to ensure that users of CCG IT systems do so in a secure, lawful and responsible manner.

- IT systems may be used for limited personal use at the discretion of an individual's manager, provided that this never interferes with CCG work, relates to a personal business interest, is unlawful or brings the CCG into disrepute
- IT 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 any way, including with viruses or by corrupting data
    - to express personal views which could be misinterpreted as those of the CCG or which are prejudicial to the interests of the organisation o to commit the organisation to purchasing or acquiring goods or services without proper authorisation. (please also refer to CCG Social Media Guidelines)
- IT systems must be locked when leaving a workstation unattended (CTRL-ALT-DEL then Enter OR Windows Key + L)
- Where users are provided with access from, or by computers for use at home, it is the user's responsibility to ensure that no unauthorised or inappropriate use is made on that computer
- Where a user has reason to believe that their password has been disclosed to others, they must change it immediately and report it to their Information Asset Owner. In addition it should be reported as a potential security incident with the IT service desk

- Users are responsible for the safe keeping of IT equipment issued for use.

1. Introduction

This document provides statements detailing Acceptable Use in relation to use of IT systems and equipment belonging Bristol, North Somerset and South Gloucestershire (CCG). It forms part of BNSSG Information Security Management System

The Information Security Management System (ISMS)

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

- sets out the governance of IT security
- provides high level policy statements on the requirements for managing IT security
- defines the roles and responsibilities for implementing the IT security policy
- Identifies key standards, processes and procedures to support the policy
- defines security architectures that encapsulate the policy and support the delivery of secure IT services

There are several policies which comprise the ISMS which include the following:

Password Policy

Clear Screen Policy

Network Security Policy

IT Disposal Policy

Anti-Virus Policy

Information Security Policy

Some of these policies which have been agreed by BNSSG govern the operation of the IT estate provided by SCW CSU.

2. Purpose

The purpose of this document is to provide clear guidance on the appropriate, safe and legal way in which users can make use of IT equipment, services and systems by:-

- ensuring users are aware of their responsibilities
- clarifying protocol regarding acceptable and unacceptable use of internet, email, network access and the use of corporate and personal IT devices to access BNSSG information systems
- ensuring CCG legal and statutory requirements are met; and protect the organisation against potential liability
- minimize risk of inadvertent, accidental or deliberate unauthorized access or disclosure
- reduce or avoid security threats by increasing awareness and disseminating good practice
- control the copying/distribution of copyrighted materials

3. Scope

This policy applies to any individuals authorised to undertake work on behalf of the CCG, and who have been provided with access to IT systems. This includes:

- directly employed staff for whom CCG has a legal responsibly
- contractors and sub-contractors
- any third party accessing CCG IT systems including volunteers
- staff covered by a letter of authority/honorary contract or work experience whilst undertaking duties on behalf of the CCG

4. Principles

- all data and information residing on CCG IT systems remains the property of the CCG at all times, unless otherwise stated
- users accept that personal use of CCG IT systems is not a right and must be exercised with discretion and moderation at all times
- users accept the CCG will not accept any liability, in part of whole, for claims arising out of personal use of CCG IT systems or information.
- CCGretains the right to:

- monitor the use of its information systems for the purpose of protecting it's legitimate concerns*, and
- prohibit personal use of information systems without warning or consultation where evidence points to a risk to BNSSG CCG including a breach of this, or any other BNSSG CCG policy

*** BNSSG CCG and/or its digital delivery partner monitors use for the prevention and remediation of cyber security issues. The CCG will only interrogate this data or monitor individual staff use when a legitimate need arises and with the approval of the Data Protection Officer**

5. Conditions of use

The CCG believes it is important to encourage the use of email, internet, and its IT systems for the benefit of the NHS community. At the same time, the CCG 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 conditions of use, along with acceptable use standards, policies and supporting guidelines listed here, are reviewed biennially.

Users should speak to their line manager if they require further advice on any aspect of complying with these statements

IT Systems Conditions of Use

All users of CCG IT systems, as a condition of use, are required to :

- ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation (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 Laws 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 SCW CSU and BNSSG 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 Email

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

- interferes with CCG work
- relates to a personal business interest
- is unlawful
- brings the CCG into disrepute or has potential to bring the CCG into disrepute

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 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 any way, including with viruses or by corrupting data
- to express personal views which could be misinterpreted as those of the 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 (such as Facebook, Twitter) are public forums so therefore must not be used for the discussion of CCG related business and / or activities, unless authorised or from a corporate account (for example, the communications and engagement team). Please refer to the CCG Social Media Guidelines for more information.

Supporting Guidance

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

6. IT Equipment

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

Users are responsible for the safe keeping of IT equipment issued to them.

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

CCG IT equipment must be returned on termination of employment or business relationship with the CCG or upon request.

Any information that needs to be shared with other CCG staff must only be shared using the CCG provided shared network folders and/or CCG provided collaborative working tools. Users must not store files or folders on their C drive or portable drives.

7. Connecting remotely and home users

Where users are provided with access to corporate IT services from home, it is the user's responsibility to ensure that no unauthorised or inappropriate use (as defined in this policy) is made from those devices used to remotely access corporate IT services.

Only remote access solutions that are provided or agreed with IT Services can be used to access CCG networks when away from CCG workplaces. Workstations which have remote access to CCG internal networks via the Internet must be protected from intrusion (for example, by locking screen or logging off when unattended, and ensuring passwords are not shared) to prevent unauthorised access to the CCG networks and systems. (SCW CSU IT support will provide advice and may supply approved solutions for use in such situations).

8. Identities and Passwords

An individual identity will be allocated to users. This means that users are accountable for all actions performed under that identity.

Passwords and, if provided, security tokens or smartcards, 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
- users must not allow others to use systems under their identity and must keep passwords/smartcards /tokenssecure
- users are accountable for all actions performed under their identity

Where a user has reason to believe that their password has been disclosed to others, they must change it immediately and must report this as a potential security incident with the IT Service Desk who will determine if any immediate action is required. The user should also report any information governance / security related incidents to their departmental information asset owner, who will make a decision as to whether the incident should be reported onto Datix. If logged on Datix, the CSU information governance (IG) team will investigate the incident

See the IT 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 BNSSG CCG 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. Managers should be

consulted for guidance . Where business requirements dictate that this is essential, the screen should be positioned or screened to ensure that the information cannot be overlooked.

9. Offensive and Inappropriate Material

The use of BNSSG 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.

10. Physical Security

Handheld and portable devices should be kept in your possession, or locked away when not in use.

Laptops and portable equipment should not be transported on car seats. Equipment should not be left in . Where for the purposes of transport or where leaving it in a vehicle is unavoidable equipment must be locked, out of sight either in the boot or a locked glove compartment.

Users must ensure that BNSSG CCG supplied workstations are installed in a physically secure part of the building to protect them from theft and inappropriate or unauthorised use.

11. Additional User Policies and Guidance

12. E-mail and Internet Monitoring Policy

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

13. Incident Reporting Guide

For the protection of 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:

- Their line manager, by phone, email or in person
- SCW CSU Service Desk

- Their departmental information asset owner, who will make a decision as to whether the incident should be reported onto Datix. If logged on Datix, the CSU IG team will investigate the incident (please refer to CCG Information Incident Management Reporting Procedure).

The following types of incidents must be reported:

- Any suspected misuse of BNSSG 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 malware infection is suspected on a workstation or server – note you must immediately turn the device off and then report it
- Where a user discovers or suspects user behaviour which does not comply with the computer condition of use or any other information security policies
- Where a user suspects 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.

14. Legal Requirements

The legal framework on which this acceptable use policy and other related information security policies are based is as follows.

All CCG staff are required to ensure compliance with Data Protection Legislation. This includes:

- 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

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality and the processing and sharing of personal data including:

- 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

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 1998
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health 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

This legislation can accessed via the following link:

http://www.legislation.gov.uk

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

15. 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 BNSSG 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 BNSSG CCG 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.

Before sending email, ensure that what is being sent is of an appropriate standard and is being distributed securely to appropriate email addresses

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

17. 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 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.

18. Third-Party Information

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

Certain information may be subject to special provisions. Please refer to the CCG's policies on Freedom of Information and also Individual Rights (which deals with Subject Access Requests

19. Roles and Responsibilities

All CCG employees, as well as any contractor, consultant or employee of a partner organisation, who are provided with access to any IT or computer service provided by the CCG must comply with these statements.

The following are also responsibilities of individuals covered by this policy:

Staff shall accept full responsibility for the security of equipment and information and information assets which are issued to them, taking necessary precautions. Devices should not be left unattended in a public place, or left in vehicles with on view, unattended or overnight.

Staff must ensure that portable computing devices (laptops, smartphones, tablets and USBs) are encrypted. Staff must not store data on portable media drives or other portable storage devices

Staff must not install any hardware or software on to the CCG devices without unless authorised and approved by IT service desk.

Staff must not change the configuration of any security settings on any CCG devices unless authorised by the IT helpdesk.

Staff must not remove or deface any asset registration number.

Staff must allow SCW IT Services access to the devices to undertake any maintenance work.

Staff should seek permission before taking any CCG IT equipment outside the United Kingdom.

Staff must not store any data on Non-SCW supplied devices.

Portable media drives should only be used to transport information when other more secure methods are not available. Information must not be stored permanently on portable devices. Where there is legitimate requirement to store data for secure transfer using portable media drive then use ONLY SCW-supplied encrypted memory stick. Do not write the password down, and if it needs to be shared with other member of staff, inform the other individual verbally.

Personal memory sticks must not be plugged into any corporate endpoints i.e. laptop, workstation, server, printer or any network equipment unless authorised by service desk.

Under no circumstances should PROTECT or RESTRICTED information be emailed to your personal non-NHSmail email address.

Home/personal computers or laptops must not be connected to the organisation's corporate network. The storage of organisation's information on personal devices is strictly prohibited.

Users must ensure that they log a call, via the Service Desk, for the disposal of any equipment capable of storing sensitive data

Users must not accept, or run, software from non-trusted sources

Users must not undertake any activities with the intention to create and/or distribute malicious programes into corporate networks of systems

Failure to fulfil responsibilities could lead to access to the IT or computer systems being withdrawn and, in the case of employees, disciplinary action taken.

Staff are not permitted to reject or disable automated security updates. Staff should ensure all portable devices are connected to CCG networks to download security patches within 30 days of the last connection or their device may be disabled.

20. Training

There is no formal training available in relation to this policy, however the CCG is required to comply with the CCG information governance staff handbook that stresses the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. As information governance is a framework drawing these requirements together, it is important that staff receive the appropriate training.

The NHS Operating Framework 'Informatics Planning' and the Data Security & Protection Toolkit training requirement requires that the CCG ensures all staff receive annual basic information governance training appropriate to their role.

On joining the organisation, CCG staff will receive a copy of the Data Security Awareness/information governance staff handbook sent by the CSU IG lead.

All staff are required to undertake information governance training annually. This should be completed through the E Learning for Health training platform: https://www.e-lfh.org.uk/ (which can be accessed through the ConsultOD Portal) or approved face-to-face information governance training delivered by the information governance team if this is available. However, new staff must complete their first training session online. This training includes elements relating to Information Security.

21. Equality impact assessment

The CCG is committed to equality, diversity and inclusion for all, as well as meeting the Public Sector Equality Duty (Equality Act 2010).

Both new policies, and existing policies when reviewed, come within the Public Sector Equality Duty. This means that policy authors must consider whether the policy will be effective for all patients and / or staff. This process is called equality impact assessment.

This policy was assessed against the SCW CSU Equality Impact Assessment tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities (see Appendix A).

The equality impact assessment highlighted that IT could be misused by an employee in order to discriminate, harass or victimise others. The policy has therefore been amended to include this as a form of misuse. Given this, the policy aims to have a positive equality impact by preventing this from happening.

22. Success Criteria / Monitoring the Effectiveness of the Policy

Adherence to this policy will be monitored via investigation and analysis of information security incidents reported via the approved incident management process. This will include the number of incidents that relate to discrimination, harassment or victimisation.

Compliance with the Data Security and Protection toolkit will be assessed by NHS Digital including a review of evidence, as part of the CCG performance assessment.

The CCG will ensure that information governance / IT security is part of its annual cycle of internal audit. The results of audits will be reported to Audit Committee.

In addition, compliance with / awareness of information governance / IT security will be monitored through the following mechanisms:

- Receipt of the IG Staff handbook confirmation slips or emails confirming that staff have received a copy of the IG staff handbook and understand their responsibilities
- Completion of induction and annual IG training
- Completion of IG modules / training relevant to the roles of the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, Information Asset Owners and Data Custodians / Information Asset Administrators
- Updates to CCG IG Group.

23. Countering Fraud

The CCG is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document

24. Review

This document may be reviewed at any time at the request of either the Staff Partnership Forum or management, or in response to changes in legislation, but will automatically be reviewed on a biennial basis.

25. References and Links to other Documents

- Legislation as listed under paragraph 4.3.1 above
- Policies / documentation as follows:
  - CCG Social Media Guidelines
  - CCG Conduct, Performance, Grievance & Absence Management Policy: Disciplinary Procedure
  - CCG Information Governance Policies
  - CCG Information Incident Management & Reporting Guidelines
  - CCG Remote Working and Portable Devices Security Policy
  - CCG IT Password Policy

26. Appendices

Equality Impact Assessment

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 (BNSSG CCG) 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
Date analysis completed
Name and signature of responsible Director
Date analysis was approved by responsible Director

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	Awareness of Policy	Launch of Policy shared at Stand Up	RH	March 20	April 20	Time on agenda
Staff	Access to policy	Upload on to Hub	RH	March 20	April 20	Comms support

End of Policy Document