INFORMATION SECURITY AND EQUIPMENT POLICY

AUGUST 2019

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

We are, we care.
Every day we are creating a healthier Hull

Name of Policy:	Information Security and Equipment Policy
Date Issued:	October 2019
Date to be reviewed:	October 2022

Policy Title:	Information Security and Equipment Policy
Supersedes: (Please List)	Information Security Policy 1.2 Computer Equipment away from the workplace Information Security Policy 2.0 Computer Equipment away from the workplace
Description of Amendment(s):	Addition of HSCIC Guidance and Caldicott 2 requirements Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation). Change in regards to mobile computer/ IT Kit.
This policy will impact on:	All Staff and relevant others
Version No:	3.0
Issued By:	Information Governance and IT Team
Author:	Information Governance and IT Team
Effective Date:	October 2019
Review Date:	October 2022

Impact Assessment Date:	October 2019	
APPROVAL RECORD		**APPROVAL RECORD**
	Integrated Audit and Governance Committee (Virtually) Integrated Audit and Governance Committee	October 2019 November 2021
Consultation:	Information Governance Steering Group	August 2019
	Relevant Others	August 2019

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by and Date
0.2	Chris Wallace	First draft for comments	
1.0	Barry Jackson	Approved version	
1.1	C Wallace	Updated layout	8 March 2016
1.2	Mark Culling	Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).	November 2017
2.0	Hayley Gillingwater	Amendments to reflect Data Protection Act 2018 & GDPR Removal of reference to IG Toolkit Inclusion of: Appropriate Usage Security of Computer Equipment Mobile Phones IAO Responsibilities / House Keeping elements	Integrated Audit and Governance Committee – October 2019 (virtually)
3.0	Hayley Gillingwater	Extension to review date	November 2021

CONTENTS

1 INTRODUCTION

Information and information systems are important assets to every organisation and it is essential to take all the necessary steps to ensure that they are comprehensively protected, available and accurate to support the operation and continued success of the CCG at all times.

The Information Security and Equipment Policy is a key component of the CCGs overall information security management framework and is designed to:

- provide a corporate framework in which security threats to our Information Systems can be identified and managed;
- illustrate the CCGs commitment to the security of information and information systems;
- provide accepted formal procedures to ensure a uniform implementation of security measures;
- introduce and formalise procedures to minimise the risk of unauthorized modification, destruction or disclosure of information; and
- align the organisation to the NHS Information Governance aims and expectations described in the Information Security Management: Code of Practice for NHS Organisations.

  Note: these objectives can only be achieved if every staff member observes the highest standards of personal, ethical and professional conduct in relation to the handling and management of information.

1.1 Requirement for Information Security and Equipment Policy

The CCG acknowledges that information is a valuable asset, therefore it is within its interest to ensure that the information it holds is suitably protected from any threat. By protecting its information the CCG is acting in the best interests of its employees and all third parties with whom information is shared whilst minimising key risks associated with information processing:

- legal action due to non-compliance with statutory and regulatory requirements
- loss of public confidence in the CCG
- contribution to clinical or corporate negligence
- loss of equipment

Key issues addressed by the Information Security and Equipment Policy are:-

- Availability - information is delivered to the right person when it is needed.
- Confidentiality - data access is confined to those with specified authority to view the data;
- Integrity - all system assets are operating correctly according to specification and in the way the current user believes them to be operating; and

The CCG intends to achieve a standard of excellence in Information Governance by ensuring all information is dealt with legally, securely, efficiently and effectively in order to support the delivery of high quality patient care, service planning and operational management. For this to be achieved information processing must comply with legislation and best practice and the CCG will establish and implement policies and procedures to ensure appropriate standards are defined, implemented and maintained.

1.2 Legal Compliance

The CCG is bound by the provisions of a number of items of legislation affecting the stewardship and control of patient and other information. The main relevant legislation is:

- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- Access to Health Records Act, 1990 (where not superseded by the Data Protection Act, 2018);
- Computer Misuse Act, 1990;
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998; and
- The Human Rights Act 1998.
- This policy describes the way in which information should be managed, in particular, the way in which personal or sensitive information should be protected. In addition to the above, other legislation can impact upon the way in which we should use personal information. This includes:
- Public Interest Disclosure Act 1998;
- Audit and Internal Control Act 1987;
- Public Health (Code of Practice) Act 1984;
- NHS (VD) Regulations 1974;
- National Health Service Act 1977;
- Human Fertilisation and Embryology Act 1990;
- Abortion Regulations 1991;
- The Terrorism Act 2000;
- Road Traffic Act 1988;
- Regulations under Health and Safety at Work Act 1974.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.Health and Social Care Act 2012 Health and Social Care Act (Safety and Quality) 2015
- Records Management Code of Practice for Health and Social Care 2016
- Much of the legislation mentioned is available in electronic format, via the Internet (www.legislation.hmso.gov.uk). In addition, the CCG is bound by the confidentiality aspects of common law and the Caldicott guidance on protection of patient information.
- As part of, and in addition to, the above legislation the CCG is required to retain all records (health and administrative) for specified periods of time. For further information on this see the Records Management Policy.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance and IT team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Bribery Act 2010

The CCG has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010.

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf.

If you require assistance in determining the implications of the Bribery Act please contact the Local Counter Fraud Specialist on telephone number 01482 866800 or email at nikki.cooper1@nhs.net Due consideration has been given to the Bribery Act 2010 in the development of this policy (or review, as appropriate) of this policy document and no specific risks were identified.

4 SCOPE

The Information Security and Equipment Policy applies to all business functions within the CCG and all third party services that provide a service on behalf of the CCG. The policy covers data, information systems, networks, physical environment and relevant people who support these functions. It relates to both manual and electronic information, whether transmitted across the N3/HSCN network, personal email addresses, skype, or telephone lines, spoken in conversations or printed as hard copy.

5 POLICY PURPOSE AND AIMS

Operating Procedures and Standards

5.1 Compliance

It is the policy of the CCG to ensure compliance, in accordance with all the legislative obligations. The CCG also requires all employees, contractors and third parties to comply with this policy and supporting standards and procedures where appropriate.

5.2 Information Security Awareness and Education

It is the responsibility of all employees' and third parties of the CCG to sustain excellent information security. To comply with this, the CCG requires all employees and contractors within scope to understand the importance of information security and be familiar with this document, and supporting documents where appropriate.

To facilitate this data security and awareness training will be included in the staff induction process and as an annual requirement in order to ensure staff awareness is refreshed and updated as necessary. This is a mandatory requirement; failure to complete data security and awareness training may result in disciplinary procedures.

5.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. In addition information security expectations of staff shall be included within appropriate job definitions.

5.4 Email and Electronic Systems

The CCG has clear standards relating to the use of e-mail, Internet and intranet and the deliberate or accidental misuse of electronic systems. The procedures cover use of any systems used to store, retrieve, manipulate and communicate information (e.g. telephone, e-mail, Skype, IT systems and the Internet). All employees and third parties are required to familiarise and adhere to them.

5.5 Access Controls

Physical Security:

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

In addition each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

In order to minimise loss of, or damage to, assets equipment will be physically protected from threats.

All staff are responsible for the physical security of assets and equipment used by them on behalf of the CCG. Appropriate physical security measures shall be put in place to secure information assets, dependant on value and sensitivity to the organisation.

All staff are responsible for ensuring that their work areas are left in a secure state when vacant.

5.6 Appropriate Usage

- Person Identifiable data must not be sent off site via e-mail unless an appropriately secure email address is used. See Appendix 1 for a definition of person identifiable data.
- Internet e-mail services of any sort are not secure and should not be used to send Person Identifiable data or any other confidential information e.g. Hotmail/Gmail
- Staff must not use the automatic forward tool where the recipient will be via a commercial ISP (Internet Service Provider) such as Hotmail, Yahoo, etc.
- Staff sending e-mail should be aware that that the addressee may not be the only person to see the e-mail.
- To restrict the possibility of viruses being transmitted to NHS computers, devices and networks, staff must not use personal computers for work-related activities unless anti-virus scanning software has been installed with the exception of secure NHS mail browser access.

- No CCG data should be stored or accessed on personal devices unless this is an operational necessity. Such cases should be discussed with the CCGs Data Protection Officer.
- If you have any issues with your computer equipment or access to data the IT supplier can be contacted via the approved process. Please note that logging an issue via the self-service portal out of hours does not guarantee that you will receive a response before the next working day.

5.7 Security of Computer Equipment:

- When you remove equipment and data from NHS premises you are responsible for ensuring its safe transportation and storage as far as is reasonably practical. Computer equipment should be kept out of sight and not be left unattended were possible and when stored in the home, windows and doors should be secured when your home is unoccupied. Computer equipment must be transported in a secure, clean environment and must not be left in a vehicle overnight. You may be held liable if you do not take reasonable precautions.
- Unless a departmental Business Continuity Plan (BCM) states you need to take devices on a more frequent basis.
  All staff issued with a work mobile phone should not leave the phone in the office – the phone can however be switched off if required.
  All staff over Band 8A or over who have been issued with mobile computing devices should not leave the devices in the office.
  In the event of a pre-emptive amber or red weather warning – Staff should use mobile technology, where issued, to be prepared to work away from the office as effectively as in the office.
- Computer equipment can be connected to a home network under remote access although computer equipment should not be used to download any files/programs for personal use.
- When working from public Wi-Fi, a secure remote access tool should be used.
- Remote access can be requested for any existing staff member or can be requested as part of the setup of a new account.
- Requests for remote access should be directed to the IT Service Desk and should originate from the Line Manager of the individual requiring the access. Once logged the IT service desk will process the request.
- Staff must ensure that data is stored in compliance with Records Management Guidance.
- Staff must ensure that no patient identifiable data is stored on their computer unless is it saved in the agreed secure area on the y-drive. Please ensure that data is never saved to the c-drive under any circumstances.
- On terminating employment, NHS computer equipment, software, data, materials and information must be returned to the line manager who will then liaise with the IT Supplier to ensure that all appropriate accounts are closed.
- Any confidential paper documents taken home must be stored in a secure manner.

There is a legal requirement for the Chief Officer to report any computer crime involving accessing illegal material to the police. Users of the Internet are committing a criminal offence by downloading illegal material and Hull Clinical Commissioning Group would be required to involve the police if such materials were found on any of its computer equipment.

5.8 Mobile Phones

In some cases, employees will be provided with a mobile phone with a tariff that has been designed to provide sufficient usage for all working requirements.

Employees must avoid use of data for personal use; however Wi-Fi is acceptable. Any use of data should not incur an additional charge to the CCG.

The CCG has adopted a 'Fair Usage' policy and as such employees will not be charged for making personal calls on the understanding that they only make these calls when essential. Mobile phone usage will be monitored on a monthly basis and excessive personal use will be investigated, with the potential for employees being charged for personal use.

Tethering should only be used when alternative options for connectivity e.g. WiFi are unavailable as it quickly uses up the data allowance, however employees are expected to tether to their mobile phone if required. If an employee feels they may require additional data allowance this should be discussed with their manager.

'All staff should adhere to the terms of use for work mobile telephone.

5.9 User Access Controls:

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.10 Computer Access Controls:

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.11 Application Access Control:

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

The CCG has a procedure outlining the control of access to its premises, physical assets and electronic networks. Procedures also cover correct use of its assets. All employees and third parties are required to acquaint themselves with these standards.

5.12 Computer and Network Procedures:

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the IT Department.

Through connection to the CCG's network it is possible to receive and forward information to other users of the network and other organisations' networks using, for example, electronic mail. Should employees receive, identify how to, or gain access to unauthorised information on any networks then this event must be reported to the IT Service Desk.

- Equipment must not be used until identified by the IT support staff that the system is ready for use.

- A security log of access to the organisations network must be maintained.
- All computer files transferred from other networks must be checked for viruses before use within the organisation.
- All employees must inform the IT Service Desk if a virus is detected or suspected immediately.
- Failure to immediately notify the CCG of a suspected virus or data breach may result in disciplinary procedures.

5.13 Information Risk Assessment and Asset Management

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the Information Asset Register and action plans shall be put in place to effectively manage identified risks. The Information Asset Register and all associated action plans shall be compiled and reviewed regularly by Information Asset Owners (IAO). Any implemented information security arrangements shall also be a regularly reviewed feature of the CCGs risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed. IAOs shall submit the risk assessment results and associated mitigation plans to the Senior Information Risk Owner for review. The IAR is sent to IAOs to be updated on a quarterly basis, IAOs are required to respond to the call for updates even if there are no changes to their assets.

5.14 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported via the CCGs Incident Management process to the Associate Director of IT.

All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

Information Governance breaches must be reported at the earliest opportunity in order that they can be investigated in a timely manner and reported to the Information Commissioner's Office (ICO) within 72 hours if required.

Staff will NOT be subject to disciplinary proceedings for basic human errors or genuine mistakes. However, failure to report known breaches will be taken seriously.

5.15 Classification of Sensitive Information – [Pending New Guidance]

The CCG will implement information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Security and Protection Toolkit to secure their NHS information assets. For more information on information classification is contained within the CCG Records Management Standard and Procedures.

5.16 Protection from Malicious Software

The CCG will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users

will not install software on the CCGs property without permission from the Associate Director of IT. Users breaching this requirement may be subject to disciplinary action.

Under the Computer Misuse Act 1990 'hacking' and the introduction of computer viruses are criminal offences. The purpose of the Act is to make provision for securing computer material against unauthorised access or modification. It makes unauthorised access to a computer, programs or data an offence.

Staff should report any viruses, suspected viruses or suspicious emails (which could contain viruses) to the IT Service Desk.

All information management and technology security (Cyber) incidents and weaknesses must be reported immediately in line with the CCG Incident Reporting Policy.

Incidents that present an immediate risk to the CCG such as viruses should also be reported to the IT Service Desk immediately.

Information Security Incidents, especially those involving the loss of sensitive or confidential data, or any incident involving unencrypted portable devices may need to be reported as a Serious Incident and/ or to the Information Commissioner via the Data Security and Protection Toolkit reporting system. See the Incident Reporting policy for more details.

There is a legal requirement to report any such serious incidents to the authorities within 72 hours.

All staff undertake appropriate annual data security training, renamed "Data Security Awareness Level 1" to reflect Data Security Standard 3 in the Caldicott 3 Review, and pass a mandatory test.

The CCG obtains regular assurance from Core IT providers that CareCert Alerts are being acted upon and are being addressed appropriately. CareCert informs organisations about cyber security vulnerabilities, mitigating risks, and reacting to cyber security threats and attacks.

5.17 User Media

The CCG will use port control software to control the use of removable media. Access to USB mass storage devices and CD/DVD writers will be restricted to approved users only.

Where removable media is received from external sources or has been used on computers systems not owned by the CCG users are required to scan the media using anti-virus software before its use.

All removable magnetic media must be encrypted. Failure to do this may result in disciplinary action.

5.18 Accreditation of Information Systems

The CCG shall ensure that all new information systems, applications and networks include a security policy and are approved by the Associate Director of IT before implementation.

System specific security policies will be developed for systems under CCG control in order to allow granularity in the security management considerations and requirements of each. This may result in

specific responsibilities being assigned and obligations communicated directly to those who use the system.

The CCG shall ensure that all new information systems, applications and networks include a Data Protection Impact Assessment (DPIA) and System Level Security Policy (SLSP) and are approved by the Information Governance Group and/or D IT before they commence operation.

When planning for, and during procurement of, new systems, it is the responsibility of the Project Manager or Lead to ensure that appropriate system security features are included within the system. As a minimum this will include a password protection feature and audit logs.

Systems and applications must be adequate for their purpose.

Software applications, upgrades and amendments must be developed in a controlled manner, documented and thoroughly tested before implementation.

Proof of ownership of software licenses must be maintained and master disks held in a secure environment in the event of necessary re-install.

Unauthorised software must not be introduced onto any system without prior authorisation from the IT Service Desk.

5.19 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Associate Director of IT or authorised officer.

5.20 Intellectual Property Rights

The CCG shall ensure that all information products are properly licensed and approved by the Associate Director of IT or suitable deputy.

Users shall not install software on the organisation's property without permission from the Associate Director of IT. Users breaching this requirement may be subject to disciplinary action.

5.21 Reporting

The Associate Director of IT will keep the Senior Leadership Team informed of the information security status of the organisation as required.

5.22 Policy Audit

This policy will be subject to regular independent audit and annual assessment in line with the completion of the Data Security and Protection Toolkit by internal and external audit.

5.23 Policy Violations

It is a condition of employment with the CCG that compliance should be maintained where appropriate with the information security management policy, and supporting standards and procedures.

If any procedures or policies are violated these will be treated as security incidents, and reported in accordance with the CCGs incident reporting procedure. Failure to comply with this policy, or supporting procedures, could result in disciplinary action.

6 ROLES / RESPONSIBILITIES / DUTIES

Information Security Responsibilities

Policy review and maintenance	Chief Finance Officer / SIRO
Approval	Integrated Audit and Governance Committee
Adoption	All staff and relevant others

Responsibility for Information Security will reside with the CCG Senior Information Risk Owner. On a day-to-day basis the Associate Director of IT will be responsible for implementing, managing, monitoring, documenting and communicating the security requirements for the organisation.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- the information security policies and procedures applicable in their work areas;
- their personal responsibilities for information security; and
- how to access advice on information security matters

All staff will comply with information security policies and procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Line managers will be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff will be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

As part of its responsibility as a service provider the IT provider, is responsible for ensuring that network computer equipment will be housed in a controlled and secure environment and protected with a combination of technical and non-technical measures. The IT department is responsible for ensuring that network backup procedures are documented and undertaken and that business continuity and disaster recovery plans are produced for the network. The IT department will provide NHS Hull CCG with regular assurance that the services supplied to the CCG comply fully with the Information Security related requirements of the Data Security and Protection Toolkit.

7 IMPLEMENTATION

The policy will be disseminated by being made available on the website and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

8 TRAINING AND AWARENESS

All staff are required to complete Data Security and Awareness Training. Additional training is available for Information Asset Owners. Staff will be made aware of the policy via the CCGs website and staff communications.

9 MONITORING AND AUDIT

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.
- The CCG has in place routines to regularly audit compliance with this and other policies. In addition the CCG reserves the right monitor activity where it suspects that there has been a breach of policy.
- The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:
- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system
- Any monitoring will be undertaken in accordance with the above act and the Human Rights Act
- It is the responsibility of all staff to ensure that the potential for security breaches does not occur as a result of their actions.
- All staff must report instances of security breaches, near misses or weaknesses through the incident reporting procedures.
- The Information Governance department will report information security incidences to the SIRO and Caldicott Guardian.
- Risk Management, Information Governance and IT will investigate all suspected/actual security breaches and report to the appropriate bodies.
- The CCG will be responsible for collating and reporting the number of breaches and ensuring actions have been taken.
- IT will, in conjunction with departments; provide advice and guidance on how to maintain security and confidentiality compliance across organisations.

Refer to the organisation's Incident Reporting Policy for further details.

10 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

11 REFERENCES

Supporting Documents and Procedures

The following documents are in support of the Information Security Policy:-

Confidentiality Audit Policy

Security Policies

Records Management Policy

Information Governance Framework and Strategy

HR / Corporate Policy Equality Impact Analysis:

Policy / Project / Function:	Information Security and Equipment Policy
Date of Analysis:	August 2019
Completed by: **(Name and Department)**	Michelle Longden, Corporate Affairs Manager Hayley Gillingwater, IG Specialist
What are the aims and intended effects of this policy, project or function?	The use of computer equipment for remote and homeworking allows the CCG ensure that staff remain interconnected and able to work from almost anywhere. The CCG has developed this policy to guide staff in working safely and complying with current Data Protection legislation and GDPR.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	This policy now incorporates elements previously included in the Computer Away from the Workplace Policy A section has been added around the use of mobile phones. Security of Computer Equipment and appropriate usage
Please list any other policies **that are related to or referred to as part of this analysis**	Remote working and homeworking Policy
Who will the policy, project or function affect?	CCG Employees and relevant others
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Information Governance Steering Group Members and relevant others have been consultation with in regards to this policy.

Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs	Remote working allows staff to continue to communicate with patients and public as appropriate for their particular role. However, there is the same need to safeguard patient identifiable data when working outside of the workplace. Staff are required to maintain consideration of equality regardless of whether they are in the workplace or working remotely. Remote working allows staff to maintain their workload and duties even if they are working remotely from home/alternative location. Remote working may also be a draw for potential employees who are looking to be able to work flexibly.

Equality Data		
Is any Equality Data available relating to the use or implementation of this policy, project or function?	Yes	☐
		☐

Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.* Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	No Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?
(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

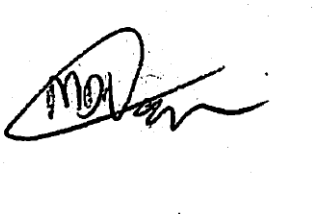
Protected Characteristic:	**No Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)**
It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy.				
Gender	✓			The application of this policy is both fair and consistent regardless of the gender and

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

				therefore does not impact on this protected characteristic
Age	✓			The application of this policy is both fair and consistent regardless of the age and therefore does not impact on this protected characteristic
Race / ethnicity / nationality			✓	The application of this policy is both fair and consistent regardless of race, ethnicity or nationality. Hull CCGs current HQ workforce data shows a higher proportion of white British staff compared to to the population in Hull. However, it is recognised that this policy is written in England and there is a risk to any member of staff whose first language is not English and support will be offered to ensure the policy is translated to the required language.
Disability	✓			The application of this policy is both fair and consistent regardless of the disability and therefore does not impact on this protected characteristic. This policy can be made available in another format, on request.
Religion or Belief	✓			The application of this policy is both fair and consistent regardless of the religion or belief and therefore does not impact on this protected characteristic
Sexual Orientation	✓			The application of this policy is both fair and consistent regardless of the sexual orientation and therefore does not impact on this protected characteristic

Pregnancy and Maternity	✓			The application of this policy is both fair and consistent regardless of pregnancy and maternity the and therefore does not impact on this protected characteristic
Transgender / Gender reassignment	✓			The application of this policy is both fair and consistent regardless of the transgender / gender/ or reassignment and therefore does not impact on this protected characteristic
Marriage or civil partnership	✓			The application of this policy is both fair and consistent regardless of the Marriage or Civil Partnership and therefore does not impact on this protected characteristic

Action Planning:				
As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?				
Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**
It is recognised that this Policy is written in English and there is therefore a risk to the staff whose first language is not English for misunderstanding.	Support will be offered to those individuals who need it and the policy could be translated if and when needed.	Communications Team	If and when required.	

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:
 **Signed:**
Date: 21.08.19