NHS
Barnsley
Clinical Commissioning Group

BARNSLEY CLINICAL COMMISSIONING GROUP'S INTERNET POLICY

January 2018

Version:	3.0
Approved By:	Governing Body
Date Approved:	February 2014 February 2016 (reviewed) January 2018 (reviewed)
Name of originator / author:	Gershon Nubour
Name of responsible committee/ individual:	Quality & Patient Safety Committee (Approval), IG Group (Review)
Name of executive lead:	Richard Walker
Date issued:	July 2018
Review Date:	2 years from approval
Target Audience:	Barnsley CCG staff

THIS POLICY HAS BEEN SUBJECT TO A FULL EQUALITY IMPACT ASSESSMENT

Amendment Log

Version No	Type of Change	Date	Description of change
DRAFT		January 2014	
1		13 February 2014	*Approved by Governing Body*
2.0	Review	Feb 2016	*References to CSU changed to EMBED* *Minor wording changes*
3.0	Review	January 2018	*Minor amendments to reflect legislation changes incl. GDPR*

Internet Policy

Contents

1. Introduction

- The internet is a useful tool that NHS Barnsley Commissioning Group (CCG) utilises in the conduct of its business. It is used for a variety of purposes including the communication of information to members of staff and the public, and to research information. The internet is also widely used by members of staff outside of work. While there are many benefits to using the internet there are also many risks to both the organisation and to individual members of staff. Staff may not be aware that breaching copyright, downloading inappropriate material, or posting inappropriate material to a social networking site outside of work time could lead to adverse consequences for both the individual member of staff and the organisation.
- This acceptable use policy is intended to enable staff and the organisation to make effective use of the internet and to avoid any adverse impact. It sets out the rules governing use of the internet both for work and personal use and it sets out CCG and staff responsibilities in relation to such use.
- It should be read in conjunction with other CCG information governance policies including, but not limited to, the Email and Copyright policies and the Confidentiality Code of Conduct. Further information can be obtained from your line manager in the first instance or the Information Governance Lead.

2. Compliance with this policy

- This policy applies to all users of CCG systems and equipment including CCG employees and non-CCG employees who work within NHS Barnsley Clinical Commissioning Group or under contract to it. This includes, but is not limited to, staff on secondment to the CCG, CSU staff, students on placement and people working in a voluntary capacity.
- For convenience, the term ‘staff’ is used in this document to refer to all those to whom the policy applies.
- All staff are expected to comply with this policy.
- This policy is based on current law, NHS Information Governance standards and accepted standards of good practice; your duty to only use the internet appropriately, stems from common law, legal obligations, staff employment contracts and professional obligations.[1]
- **Any breaches of this policy will be fully investigated in accordance with CCG procedures and, if appropriate, may result in your employment or association with the CCG being terminated. It may also bring into question your professional registration[2] and could result in disciplinary, civil or criminal proceedings. Any cases of suspected fraud will be referred to the Trust’s Counter Fraud Specialist for further investigation which may result in criminal sanction.**
- If there is anything that isn’t clear or which you do not understand in this policy you must contact your line manager, in the first instance, or the Information Governance Lead for further information

[1] For example, with the General Medical Council, Nursing and Midwifery Council or Health Professions Council

[2] See note 1 above

- Please note that the procedures and policies outlined in this policy and any related policy may be changed at any time. You will be alerted to this via established CCG communication routes such as team brief, weekly and monthly round up, intranet and internet.

3. Generic Responsibilities of Staff and the CCG

- All managers are responsible for ensuring that the staff they manage are aware of the Internet Acceptable Use policy and their individual responsibility for complying with it. They should ensure their staff are equipped to fulfil those responsibilities; this will include covering it at local induction and by identifying and meeting specific and generic training needs through personal development plans.
- Managers should ensure **ALL** new staff have signed the Confidentiality and Information Security declaration.[3] Managers are required to countersign this declaration to indicate that they have checked that the member of staff has read the relevant information governance policies and has had an opportunity to ask questions about anything they do not understand.
- Senior managers should ensure that managers within their Service are aware of their responsibilities in relation to informing staff about acceptable standards of information governance.
- All staff must ensure that they are aware of the requirements and standards of behaviour that apply and comply.
- All staff are responsible for reporting information incidents and near misses, including breaches of this policy, using the CCG's Incident Reporting Policy. The CCG's incident reporting process can be obtained from line managers in the first instance. Further information can be obtained from the Risk Advisor or Information Governance Lead.
- The CCG's Information Governance Group is responsible for overseeing the implementation of this Internet Acceptable Use Policy including monitoring compliance. It is responsible for ensuring it is reviewed periodically.

[3] The declaration should be signed by ALL staff who have access to CCG information, that is, ALL staff who work at the CCG and not only those who have access to the CCG network.

4. CCG Responsibilities and Rights

4.1 Access to and use of electronic systems

- The CCG provides access to electronic systems to employees and authorised non-CCG employees only for use in their:
  - Work duties
  - Work related educational purposes
  - Work related research purposes
- The CCG allows limited personal use of the internet in the users own time and only where it does not interfere with their work duties.
- The CCG reserves the right to prevent access to any internet sites it considers inappropriate and detrimental to CCG business.

4.2 Ensuring integrity of the system

- The CCG monitors use of the internet in line with legislation, guidance and CCG policy.
- The CCG reserves the right to remove or amend access to the internet at any time in order to protect and preserve the integrity and security of the system.

4.3 Monitoring

- All internet activity on CCG systems is logged automatically.
- Monitoring logs are audited periodically.
- Any monitoring will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, Telecommunications (Lawful Business Practice Practice) (Interception of Communications) Regulations 2000, the Data Protection Act, The General Data Protection Regulation, the Human Rights Act 1998 and CCG policy on monitoring and privacy.

5. User Rights and Responsibilities

5.1 Security

Users must:

- Lock their workstation when not in attendance for a period of time. To automatically lock the PC press the ‘windows’ and ‘L’ keys at the same time or press ctrl–alt–del AND then choose ‘lock computer’.
- Take care when accessing external sites. Some internet sites may be malicious or may have been compromised. Such sites may attempt introduce viruses, take over your PC or introduce ransomware into the network.
- Take care when posting information to internet sites. Information posted may be harvested for inappropriate and illegal activities such as sending spam emails; identity theft and hacking attempts.

5.2 Restrictions on using the internet

When accessing the internet, users must not:

- Use the internet for any purpose that conflicts with any CCG Policy, Code of Conduct or their Contract of Employment when using the internet for both work and personal use. (For example, this policy, and policies around equality and anti-harassment.)
- Use the internet to conduct private or freelance work for the purpose of commercial gain.
- Use the internet to create, hold, transmit or view material that has an obscene, pornographic or sexually offensive content (other than for properly authorised and lawful health care work or research).
- Use the internet to create, hold, transmit or view material that has an offensive (for example, racist, sexist, homophobic), defamatory, harassing or otherwise illegal content.
- Use the internet to make untrue, inaccurate, misleading or offensive statements about any person or organisation.
- Download or install any unauthorised software on CCG equipment without prior authorisation from IT services.

5.3 Blogging and social networking

- Social networking includes but is not limited to: blogs, online discussion forums, collaborative spaces and media sharing services. Examples are Blogger, Instagram, Facebook and Twitter. While this media has many benefits it also presents risks to the individual and the CCG, particularly due to its widespread use outside of work and the fact that social computing can blur the boundary between work and personal life. As an informal method of communication it is easy to publish content that you may later regret and which may not be appropriate in a work context. Such information may end up having a much wider audience than you anticipated which cannot later be retracted. You should think carefully about what you publish even outside of work because inappropriate use could lead to disciplinary action.
- The use of social networking or blogging media at work, where you are representing the CCG in an official capacity, requires the prior approval of NHS Barnsley Clinical Commissioning Group Communications Department. Care should be taken to use such media in a professional manner. (Contact the IT Department for technical support, for example, if access to a site is blocked.)
- Staff should take care to use social networking services, whether for work purposes or personal use, in a manner that is consistent with the terms and conditions of their employment or association with the CCG. For example, individuals should not post content that breaches confidentiality, contains inappropriate comments about colleagues or service users, is abusive or hateful or would potentially cause embarrassment or detrimentally affect the reputation of the CCG. In addition, where appropriate, individuals should identify that any views expressed are their own and not those of their employer.
- Failure to adhere to such guidance may result in the individual being subject to disciplinary procedures.

5.4 Copyright

No member of staff shall infringe copyright in copyright works stored on internet sites. Staff should note that downloading copyright text or images from an internet site without permission may constitute infringement of copyright even if it is not the intention to republish such works.

- Staff must **always** check copyright notices on websites
- Staff may not copy images, other electronic media or software without permission
- Staff must not download and install any software onto work equipment without prior approval of the IT Department
- Staff must not copy any software installed on work equipment for any purpose without prior permission of the IT Department
- Any employee found copying software and other media such as DVDs/CDs illegally will be subject to disciplinary procedures
- Non-work related media files such as mp3 or video files should not be stored on CCG computers
- Staff must not download and print material for commercial purposes

Further information about copyright can be obtained from EMBED's Knowledge Services Manager.

5.5 Inadvertent misuse of the internet

- A user who inadvertently accesses a site which contains material that is unacceptable and inappropriate, as specified above, must disconnect from it immediately and inform the IT Service Desk.

5.6 Further Information

- Further information can be obtained from the CCG's Information Governance Lead.
- Questions about the use of the system or any problems in accessing the internet should be directed to the IT Service Desk during opening hours. There is no out of hours or home support.

Equality Impact Assessment

Title of policy or service:	Internet Policy	
Name and role of officer/s completing the assessment:	Gershon Nubour	
Date of assessment:	12 July 2018	
Type of EIA completed:	**Initial EIA 'Screening'** ☒ ***or*** **'Full' EIA process** ☐	*(select one option)*

1. Outline	
Give a brief summary of your policy or service • including partners, national or regional	• It is intended to enable staff and the organisation to make effective use of the internet and to avoid any adverse impact. • It sets out the rules governing use of the internet both for work and personal use and CCG and staff responsibilities in relation to such use.
What Outcomes do you want to achieve	• Risk Reduction to CCG from hacking, malware and data loss when staff use the internet. • Clear understanding from staff of expected standards of behaviour when online.
Give details of evidence, data or research used to inform the analysis of impact	A draft of this policy has been circulated for review by the following:- • BCCGs Information Governance Group, • BCCGs Quality Patient Safety Committee, The final policy has been signed off by BCCGs Chief Nurse, the Head of Governance and Assurance and the Information Governance Manager (eMBED)

Give details of all consultation and engagement activities used to inform the analysis of impact	As above

Identifying impact:

- **Positive Impact:** will actively promote the standards and values of the CCG.
- **Neutral Impact:** where there are no notable consequences for any group;
- **Negative Impact:** negative or adverse impact: causes or fails to mitigate unacceptable behaviour. If such an impact is identified, the EIA should ensure, that as far as possible, it is eliminated, minimised or counter balanced by other measures. This may result in a 'full' EIA process.

2. Gathering of Information

This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.

(Please complete each area)	**What key impact have you identified?**			**For impact identified (either positive or negative) give details below:**	
	Positive Impact	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	☒	☐		
Age	☐	☒	☐		
Carers	☐	☒	☐		
Disability	☐	☒	☐		
Sex	☐	☒	☐		

Race	☐	☒	☐		
Religion or Belief	☐	☒	☐		
Sexual Orientation	☐	☒	☐		
Gender Reassignment	☐	☒	☐		
Pregnancy and Maternity	☐	☒	☐		
Marriage and Civil Partnership (only eliminating discrimination)	☐	☒	☐		
Other Relevant Groups	☐	☒	☐		
HR Policies Only:	☐	☐	☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take, please transfer them to the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**

4. Monitoring, Review and Publication			
When will the proposal be reviewed and by whom?	The EIA will be reviewed when the policy is reviewed. The Head of Assurance is responsible for ensuring the review takes place.		
Lead / Reviewing Officer:	Richard Walker	**Date of next Review:**	January 2020

Once completed, this form **must** be emailed to the Equality Lead barnsleyccg.equality@nhs.net for sign off:

Equality Lead signature:
Date: