# INTERNET AND SOCIAL MEDIA POLICY

<table>
<thead>
<tr>
<th>Version:</th>
<th>1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratified by:</td>
<td>Quality and Performance Committee</td>
</tr>
<tr>
<td>Date ratified:</td>
<td>12th July 2017</td>
</tr>
<tr>
<td>Name &amp; Title of originator/author:</td>
<td>John Robinson, Senior Information Governance Specialist (eMBED Health Consortium)</td>
</tr>
<tr>
<td>Name of responsible committee/individual:</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Date issued:</td>
<td>14th July 2017</td>
</tr>
<tr>
<td>Review date:</td>
<td>14th July 2019</td>
</tr>
<tr>
<td>Target audience:</td>
<td>All staff</td>
</tr>
</tbody>
</table>
Equality Statement

This policy applies to all employees, Joint Governing Body of NHS Leeds Clinical Commissioning Groups (CCGs) Partnership (Governing Body) irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. INTRODUCTION ................................................................. 4
2. AIMS .................................................................................. 4
3. SCOPE .................................................................................. 4
4. ACCOUNTABILITY AND RESPONSIBILITIES .................................. 5
5. DEFINITION OF TERMS ............................................................. 6
6. OBTAINING ACCESS TO THE CCG-PROVIDED INTERNET ............. 6
7. INTERNET USAGE ...................................................................... 7
   7.1 Blocking Sites ................................................................. 7
   7.2 Personal Use ................................................................. 7
   7.3 Acceptable Use .................................................................. 8
   7.4 Unacceptable Use ............................................................ 9
   7.5 Monitoring of Internet Use .................................................. 9
8. SOCIAL MEDIA ........................................................................ 10
   8.1 Social Media for Work Purposes ........................................... 10
   8.2 Personal Use of Social Media .............................................. 11
9. RISK AND PRIVACY RISK ASSESSMENT .................................... 12
10. INCIDENT REPORTING ............................................................. 12
11. RELATED LAW ...................................................................... 12
   11.1 Data Protection Act 1998 ..................................................... 12
   11.2 Common Law Duty of Confidentiality ................................... 13
   11.3 Freedom of Information Act 2000 ......................................... 13
   11.4 The Public Interest Disclosure Act 1998 .................................. 13
   11.5 Human Rights Act 1998 ..................................................... 13
   11.6 Computer Misuse Act 1990 ................................................. 13
11.7 Copyright, Designs and Patient’s Act 1998 (as amended by the Copyright Computer Programs Regulations 1992) ....................................................... 14
12. TRAINING ............................................................................................... 14
13. IMPLEMENTATION AND DISSEMINATION ........................................... 14
14. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY .... 14
15. COPYRIGHT ............................................................................................. 14
16. ADVICE .................................................................................................... 15
17. ASSOCIATED DOCUMENTS .................................................................... 15
   17.1 Core Information Governance Polices .................................................. 15
   17.2 Other Related Documents .................................................................. 15
Appendix: Internet Access Agreement ............................................................. 16
1. INTRODUCTION

The Leeds CCGs recognise that the use of the Internet is an essential tool that assists the organisation in conducting its business. Additionally, the CCGs recognises that as well as general internet use, there is an increasing use of social media throughout all sectors of society. This includes NHS organisations who are utilising social media to engage with stakeholders. CCG staff may also access social media for personal use outside of their work hours and the CCGs acknowledges the benefits of a more flexible approach to Internet and social media access. Nevertheless where staff do access the Internet and social media, they need to be aware of any implications and impact on themselves, the CCGs and wider NHS where they choose to discuss or post information about work related matters.

While there are many benefits to using the internet and social media, there can be risks associated with its use. For instance, staff may not be aware that breaching copyrights, downloading inappropriate material and posting inappropriate material, referencing individuals, even outside of working hours, could have adverse implications for both the organisation and the individual involved. This policy sets out the guidelines and parameters for employees when using the internet and social media for both work and personal use which will enable them to make effective use of technology for the benefit of the CCGs and its organisational aims and avoid any adverse impact.

Specific legislation will affect how staff use internet and social media which staff need to be aware of. The current key laws and how it can affect usage is set out in Section 11: Related Law.

2. AIMS

The aim of the policy is to ensure that:
- Employees understand their obligations and responsibilities with regard to use of internet and social media.
- Employees understand how certain legislation (such as the Data Protection Act) places obligations on the CCGs and its employees as to how information held by the CCGs can be used on the internet and social media.

3. SCOPE

This policy must be followed by all staff who work for or on behalf of the CCGs including those on temporary or honorary contracts, secondments, volunteers, pool staff, Board members, students, partner CCGs and eMBED Health Consortium staff working for the CCGs. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

The Internet is a general term that covers access to numerous servers and computer systems worldwide. Such systems include the World Wide Web (www) and NHS N3 web sites (prefixied nww) as well as any other services that are or may become accessible using internet technology connected to the CCGs.
Network.

The CCGs currently uses the N3/Health and Social Care Network – HSCN) infrastructure to access these systems and as such is bound by the Statement of Compliance.

The policy covers all equipment used to access internet and social media including computers, laptops, tablets, mobile phones and Bring Your Own Devices (BYODs).

The policy also covers any internet service accessed from CCGs equipment. This includes staff conduct both on and off site, whilst using such services.

Failure to adhere to this policy will be fully investigated in accordance with CCGs procedures and, if appropriate, may result in disciplinary, civil and/or criminal proceedings (including potential dismissal or termination of association with the CCGs) and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

If there are any issues that staff believe to be unclear about or that do not understand about this policy, they must contact their Line Manager in the first instance (or the Senior Information Governance Specialist for the CCG).

Any changes or reviews to this or any other policy will be notified to staff via established communications routes such as email, team brief, newsletters, internet and the intranet.

4. ACCOUNTABILITY AND RESPONSIBILITIES

There are a number of key information governance roles and bodies that the CCG needs to have in place as part of its Information Governance Framework, these are:

- Governing Body
- Quality and Performance Committee
- Accountable Officer
- Senior Information Risk Owner
- Caldicott Guardian
- Information Asset Owner
- Information Asset Administrator
- Heads of Service
- All employees

The accountability and responsibilities of staff are set out in more detail in the Information Governance Strategic Vision, Policy and Framework which must be read in conjunction with this policy.

All employees are personally responsible for compliance with the law in relation to their use of internet and social media that involves the use of work derived information. More specific usage requirements in terms of internet and social
media usage are outlined in Sections 7 and 8 of the policy.

All Managers are responsible for ensuring that the staff they manage are aware of this policy and of their individual responsibilities in respect of this policy. Managers must ensure that their staff have signed the Internet Access Agreement (see Appendix) and are up to date with all Information Governance training.

All staff are responsible for reporting information incidents and near misses including breaches of this policy, using the CCG Incident Management Policy.

5. DEFINITION OF TERMS

Social Media
This is the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others who often share the same community interests.

Blog
Is a type of website, maintained by an individual with regular entries by way of a commentary. It can also mean to maintain or add content to a blog. Visitors can add comments or messages to the blogs.

Multimedia
The use of computers to present text, graphics, video, animation, and sound in an integrated way.

Streaming
Streaming or media streaming is a technique for transferring data so that it can be processed as a steady and continuous stream.

Twitter
Twitter is a vast, web-based messaging network, where each ‘tweet’ is a single message.

YouTube
A free website devoted to viewing, sharing and commenting on video clips.

Facebook
Facebook is a social utility that connects people with friends and others who work, study and live around them.

Spam and junk mail
Unsolicited commercial webmail, chain letters or advertisements.

6. OBTAINING ACCESS TO THE CCG-PROVIDED INTERNET

There is a formal, documented user registration and de-registration procedure for access to the network. New users requiring access the Internet as part of their role will be provided with a copy of this policy and Internet Access Agreement (see
Appendix A) in which the new user must read then sign to declare they have read and understood the policy.

New users will be issued with a username and password for access to the CCG network. Employees must not share their password with other members of staff.

Passwords shared with members of staff could lead to disciplinary proceedings.

7. INTERNET USAGE

The primary purpose for CCG-provided internet access is for business related matters. However, this policy describes how the Internet may be used reasonably for other purposes to a limited degree.

The reasonable use of the internet is very subjective and inevitably leads to differing interpretations of what is considered acceptable and reasonable. The guidelines outlined in this policy therefore are to provide a yardstick for what is deemed to be reasonable and acceptable from a performance management perspective.

7.1 Blocking Sites

Specific sites will have been blocked for purposes relating to security, network performance and confidentiality of CCGs information and to prevent access to sites that contain illegal content.

The list, nature and range of blocked sites is determined by the CCG’s Senior Management Team, having consulted with staff and with advice from the Senior Information Risk Owner and the Leeds CCGs Information Governance Committee and our web filtering/monitoring service provider.

Blocked sites may include those that provide file transfers or storage. Any transfer or storage of personal and sensitive personal data must comply with CCGs policy requirements and legislation and be reviewed through the Privacy Impact Assessment Procedure.

7.2 Personal Use

The CCGs accepts that employees may wish to use the internet for personal use while accessing the CCG network or using their personal mobile devices and/or smartphones.

Any such use of the Internet does not contribute to an employees contracted hours.

This usage will be permissible for reasonable periods in the following times:

- In their lunch break
- Outside core working hours

The internet may be used at other times on an exception basis, subject to the
consent of the individual’s Line Manager. Any such use will be within the constraints described in the Policy. It must be noted that the overriding principle is that CCG-provided internet usage is for business purposes and that personal usage involving CCG equipment must not have an adverse effect on the operation of CCG business e.g. taking up undue ‘bandwidth’, or attempting to involve other members of staff who are currently working.

The types of sites permitted and not permitted are listed below in sections 7.3 and 7.4.

Where a staff member may exceptionally take up a long period of time browsing the Internet for personal purposes while at work, they should inform their line manager and ensure that they have their Manager’s explicit support. As a rule of thumb continuous personal use of more than one hour would fall into this category. This would include “tabbing” in and out of internet sites (including social media sites) for personal use over such a period.

Staff must avoid being drawn into spending time on social media during work hours. It can be tempting to check for responses to a post or comment, and easy to be drawn into prolonged discussions. Even quick checks on websites can interrupt concentration and affect work performance. Staff are responsible for being aware of such issues and exercising self-discipline, but may discuss any difficulties with their line manager.

Internet usage on CCG-provided facilities is automatically logged and may be monitored, which may be used to detect and/or investigate inappropriate use (see Section 7.5: Monitoring of Internet use).

### 7.3 Acceptable Use

- Internet access related to undertaking work duties such as:
  - Accessing key NHS systems
  - Accessing and sharing work related information with CCG staff and partner organisations
  - Educational, developmental or research purposes
  - Obtaining health service information
  - Professional and Personal Development and accreditation as per an agreed Personal Development Review with the users line manager
  - Accessing news sites to be stay informed about the latest NHS (and related) information
  - Using communications tools to perform CCG communications and engagement activities
- Accessing the internet for personal use on CCG owned equipment in line with conditions set out in section 7.2, and excluding sites and usage set out in 7.4.
- Streaming information for work related purposes.
- Downloading and updating software with authorisation from IT Services.
7.4 Unacceptable Use

- Accessing, creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material.
- Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.
- Accessing, creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user’s data or hardware.
- Creating or transmitting junk-mail or spam. This means unsolicited commercial webmail, chain letters or advertisements.
- Using the Internet to conduct private or freelance business for the purpose of commercial gain.
- Downloading streaming video or audio for entertainment purposes.
- Creating, downloading or transmitting data or material that infringes or breaches copyright.
- Accessing sites that involve:
  - Gambling
  - Auctioning/Buying/Selling
  - Dating
  - Playing online games
  - Radicalisation
  - Grooming
- Arranging independent access to the internet through a Virtual Private Network (VPN).
- Downloading or installing any unauthorised software on CCG equipment without prior authorisation from IT services.
- The downloading and use of any unlicensed software (including computer games), and any downloading of data/programs for purposes not consistent with service use. This also applies to any software brought in from home.
- Deliberate activities with any of the following characteristics :-
  - Wasting staff effort
  - Unduly using up network resources
  - Violating the privacy of other users
  - Disrupting the work of other users
- Using unauthorised file sharing sites to transfer or hold CCG personal or confidential information (see section 7.1).

7.5 Monitoring of Internet Use

Staff need to be aware that Internet traffic on CCG-provide Internet facilities is logged automatically, this includes each site a user visits, with the time visited and pages viewed. These logs may be audited and, where any inappropriate usage/patterns are identified, disciplinary action could be taken and referral to the relevant regulatory body as well as the potential for criminal investigation/prosecution (see Section 11: Related law).
If you unintentionally access, download, or transmit any information or images that are in breach of this policy then please report this to your line manager, the IT Service Desk and complete an incident form in line with CCG policies. This is to ensure that it does not result in disciplinary procedure where the breach of policy was accidental / unintended.

**Data Protection Statement**

Information recorded as part of this automated monitoring process includes user identification, domain names of websites visited, duration of visits, and non-business files downloaded from the internet. Staff should be aware that this monitoring may reveal sensitive data about them, for example visits to websites which details the activities of a particular political party or religious group might indicate the political opinion or religious belief of that staff member, or self-help or health advice sites might identify a physical or mental health condition. By carrying out such activities using the CCG internet access facilities, staff are agreeing to the CCG being party to any sensitive personal data about them, which may be recorded as part of the above monitoring.

Staff who wish to safeguard against the potential of sensitive information via the monitoring process must take responsibility for maintenance of their own personal privacy by not using the CCG network to access this type of information.

8. SOCIAL MEDIA

8.1 Social Media for Work Purposes

The term Social Media encompasses a variety of internet platforms (such platforms as Twitter, Facebook, YouTube, Blogs and forums) which allow individuals and organisations to publish, and share information and comments online. It enables individuals to become part of different networks of people with similar interests. For some platforms this is done so without the influence of an organisation, 'state' or editor.

The CCG recognises that social media is a platform which will allow it to interact with stakeholders in order to enhance its profile, provide information about the role and aims of the organisation, make professional and developmental contacts, and to gauge and understand the views of stakeholders such as patients.

There are risks, however, associated with the use social media. Where staff use social media sites for work purposes (or in personal use where that may have an impact on the CCG) they must do so in compliance with related law e.g. ensure CCG held personal and confidential information is secure, that copyright is not infringed and defamation of character does not occur.

When participating in social media networks for work purposes:

- Staff must be clear that they are representing the CCG.
- Staff can provide their name and role at the CCG but should not provide
personal details about themselves such as date or birth, home address etc.

- Staff should only cover areas in which they are expert.
- When intending to publish official CCG content staff need ensure that there is authorisation to do so (the same as when information is posted on the CCG website).

Where considering participating in or setting up a CCG social media presence:

- Staff must discuss the proposal with their line manager and the Communications Team in the first instance, to ensure that it is appropriate and in line with the organisation’s communications strategy.
- Staff need to have an idea of what they are trying to achieve and how to link this activity to the overall business plan for a programme or business area. This may involve putting forward a Project Initiation Document.
- Staff must ensure that they have the explicit approval of the CCG via Line Managers or the Communications Team to represent the CCG on the matter.

8.2 Personal Use of Social Media

The CCG recognises that staff may wish to participate in social media sites out of work time for personal use. However, when someone clearly identifies their association with the CCG and discusses their work or work-related matters, they are expected to behave appropriately, and in ways that are consistent with the CCG’s values and policies. The same conditions for confidentiality and security of information (where it relates to CCG information) will apply for personal use as it does when using the information in a work setting. If an employee makes reference, in a personal capacity, to the CCG or the wider NHS then this must be clearly distinguishable from their professional capacity.

When accessing social media for personal use where comments or information relate to the CCG work, the following apply:

- Staff must remember that these sites are a public forum and form part of a network. At no time should staff assume that any entries will remain private. Staff are reminded that they are personally responsible for the content published and that these items may remain on these sites for a very long time.
- Staff should not post defamatory, derogatory or offensive comments on the internet about colleagues, patients, their work or the CCG.
- Staff must not reveal any confidential or personal information about patients, or staff.
- Where photos of other staff are taken informally at work or outside of the work environment such as social occasions and a staff member is then intending to share on social media, it should be done with consideration taking into account the perceptions of those other staff as to the level of circulation of those photos. Consent must be sought and given prior to capturing any images of employees – any potential sharing or wider use will need to be identified as part of this process. Any content pertaining to another member of staff should be removed if requested to do so.
- Likewise, photographs of staff taken with their consent and for work purposes
should only be used for that specific purpose and situation (e.g. for a staff publication), should not be published outside of that agreed area. The artist/publisher should be clearly acknowledged. It is noted, however, that where a document (such as a staff publication) has been published in the public domain already it would possible to link to the publication – this does not allow for the content to be reused for different purposes.

- Staff should not impersonate another colleague on social networking sites/forums.

9. RISK AND PRIVACY RISK ASSESSMENT

When considering a new project involving: web access, establishing a social media presence or participating in new social media networks – they should be risk assessed. Staff need to address any privacy concerns of implementing the new project or process and a Privacy Impact Assessment (PIA) should be used.

A PIA will:

- Identify privacy risks to individuals
- Protect the CCG’s reputation
- Ensure person-identifiable data is being processed safely
- Foresee problems and negotiate solutions

The CCG procedure for Privacy Impact Assessments should be followed.

10. INCIDENT REPORTING

All actual, potential or suspected incidents involving use of the internet or social media need to be documented in line with the CCG’s Incident Reporting Policy.

Incident meeting the criteria of a Serious Incidents Requiring Investigation (SIRI) level 2 or a Cyber Security Serious Incidents Requiring Investigation need to be entered on the Incident reporting Module of the Information Governance Toolkit.

11. RELATED LAW

Some of the key legislation and common law is set out below and how it may affect use of information the internet and social media. Employees need to be aware of legal requirements for both work, and personal use (where it may have an impact on the CCG).

11.1 Data Protection Act 1998

Sets out the conditions for the processing of personal information by organisations and individuals. Employees need to be aware that any use of personal information stemming from work related business can only be used where conditions of the Act can be met.
11.2 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:

- Where the individual to whom the information relates has consented
- Where disclosure is in the public interest; and
- Where there is a legal duty to do so, for example a court order.

Confidential information could relate to personal information of an individual or information contained in a business related document e.g. contract.

11.3 Freedom of Information Act 2000

Allows the right of access to anyone to recorded information held by a public authority (such as a CCG) via a request for specific information or through accessing information via the public authority’s publication scheme. Release of information is subject to exemptions and conditions of the Act.

All staff, however, should consider all information which they come into contact with through the course of their work as confidential and its usage and any disclosure would be in line with agreed duties and for authorised work purposes. This would be the case regardless of whether the information may be made available through the Freedom of Information Act. For release of CCG held information, the CCG already has in place the processes for making information available through the request procedure or has made certain information publicly accessible through the CCG Publication Scheme.

It should be noted, however, that where a document has been published in the public domain already it would possible to link to the publication.

11.4 The Public Interest Disclosure Act 1998

This Act allows employees to voice authentic concerns about misconduct and malpractice without receiving penalties such as dismissal, victimisation, or denial of promotion, facilities or training opportunities.

11.5 Human Rights Act 1998

Article 8 of the Act provides a right of privacy for individuals. In complying with the Act, public authorities (to which the Act applies) such as the CCG need to ensure that personal and confidential information is not disclosed into the public domain (unless a legal justification exists to do so).

11.6 Computer Misuse Act 1990

Under this Act it is an offence to have unauthorised access to computer material or to undertake unauthorised modification of programs or data on a computer.
11.7 Copyright, Designs and Patient's Act 1998 (as amended by the Copyright Computer Programs Regulations 1992)

See Section 15: Copyright.

12. TRAINING

There are information governance implications involved in the use of internet and social media especially in terms of the confidentiality and security and legal use of information, therefore, it is important that staff understand their information governance responsibilities. The Information Governance Toolkit requires that all staff must undergo information governance training annually. All staff will receive information governance training via the CCG’s Statutory and Mandatory Training Programme. Managers must actively ensure that all staff undertake and successfully complete the mandatory information governance training.

The Information Governance training requirements are captured within the Information Governance Training Strategy.

13. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Audit and Governance Committee this policy will be disseminated to staff via the CCG’s intranet and communication through in-house staff briefings.

This policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

14. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the Information Governance Toolkit (IGT), will be undertaken each year. The IGT includes requirements relating to confidentiality, data protection, security of and access to information. Incidents are reported and all serious information governance issues must be reported by the SIRO at Governing Body level and in Annual Reports.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the Report NHS Fraud website or telephoning 08000 28 40 60.

15. 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.
16. ADVICE

Advice and guidance on any matters stemming from the policy can be obtained by contacting your line manager or through the IG service provided by Embed: embed.infogov@nhs.net

17. ASSOCIATED DOCUMENTS

17.1 Core Information Governance Policies

This policy should be read in conjunction with the six core Information Governance Policies:

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Confidentiality and Data Protection Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Records Management and Information Lifecycle Policy

And in particular the Confidentiality and Data Protection Policy, and Information Security Policy which set out the rules for security and confidentiality of information.

17.2 Other Related Documents

- Incident Reporting Policy
- Risk Management Policy
- Email Policy
- Disciplinary Policy
- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Communications Strategy
Appendix: Internet Access Agreement

I have received a copy of the Internet and Social Media Policy. I understand the terms of this policy and agree to abide by them. I realise the CCG Network Security Software may record for management use the Internet address of any site that I visit and keep a record of any network activity. I am aware that any deliberate violation of this policy may lead to disciplinary action, including dismissal or criminal prosecution.

<table>
<thead>
<tr>
<th>Name (please print)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td>Designation</td>
<td></td>
</tr>
<tr>
<td>Work Location (e.g.</td>
<td>Leafield House, Thorpe Park, WIRA House)</td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
</tbody>
</table>

**Line Manager**

<table>
<thead>
<tr>
<th>Name (please print)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td>Designation</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
</tbody>
</table>

**Please return signed form to the Leeds CCG Help Desk:**

By scan (via NHSmail) to LeedsCCG.Helpdesk@nhs.net