NHS
Wakefield
Clinical Commissioning Group

Electronic Communication and Social Media Policy and Procedure

Version: 2.0

Committee Approved by: Integrated Governance Committee

Date Approved: May 2019

Author: Senior Communications Officer

Responsible Directorate: Corporate Affairs

Date issued: November 2019

Review date: April 2020

Review and Amendment Log / Version Control Sheet

Responsible Officer:	Ruth Unwin, Director of Corporate Affairs
Clinical Lead (where appropriate):	Dr Clive Harries, Caldicott Guardian
Author:	Communications and Information Governance Teams
Date Approved:	16th May 2019
Committee:	Integrated Governance Committee
Version:	2.0
Review Date:	April 2020

Version History

Version no.	Date	Author	Description	Circulation
1.0	April 2018	Senior Information Governance Officer	Approved version (April – December 2018)	All staff
1.1	December 2018	Senior Communications Officer	Enhancements to policy and procedural content relating to text messaging and social media.	Integrated Governance Committee
1.2	May 2019	Information Governance Manager	Policy and procedural amendments to support the CCGs move to NHS Mail as its primary email platform and closure of the GCSX secure email service.	Integrated Governance Committee
2.0	May 2019	Information Governance Manager	Approved by Integrated Governance Committee 16th May 2019	Integrated Governance Committee

CONTENTS **Page**

Appendices

1.0 Introduction

NHS Wakefield CCG recognises that electronic communication (including social media) is now the usual and preferred method of giving and receiving information in the workplace.

We are committed to making the best use of all available technology to improve the way we work and our ability to communicate and interact with the different communities we serve.

This policy and procedure is written to guide and support staff and Governing Body members including those on temporary or honorary contracts, secondments, pool staff, students and those staff in organisations hosted by NHS Wakefield CCG, on the explicit understanding that they will make both responsible and reasonable use of access to email, the internet and social media. Inappropriate use or excessive personal use in work time will be managed through the Disciplinary Policy and Procedure and may lead to appropriate disciplinary action being taken.

This policy clarifies expectations of NHS Wakefield CCG staff and associates when using social media for both business and personal use. It also focuses on the requirements of staff when using NHS Wakefield CCG's IT systems including email and internet.

2.0 Aims and Objectives

The aim of the Electronic Communication and Social Media Policy and Procedure is to ensure all staff, Governing Body members and associates understand the principles for using email, the internet and social media in a lawful and responsible way.

Additionally, the aim is to give best practice guidance on using e-communication tools safely and effectively at work and at home. The objective is to make sure that everyone connected with NHS Wakefield CCG uses electronic communication and social media at work (and at home) in a way that protects the CCG and themselves from legal consequences including breach of confidentiality, cyber-crime and reputational damage.

3.0 Scope of the Policy and Procedure

This policy and procedure must be read, understood and acted on by everyone who works for, is associated with and represents NHS Wakefield CCG, including Governing Body members, hosted organisations, those on temporary or honorary contracts, secondments, agency staff, students and independent contractors.

4.0 Accountability

4.1 Integrated Governance Committee

The Integrated Governance Committee is responsible for making sure that the necessary support, resources and controls are in place so that individuals can use electronic communication and social media safely and effectively. The Integrated Governance Committee is also responsible for reviewing the Electronic Communication and Social Media Policy and Procedure.

4.2 Chief Officer

The Chief Officer has organisational responsibility for information governance and communications, delegated on a day-to-day operational level to the Director of Corporate Affairs. This includes making sure the organisation has appropriate systems and policies in place to maintain the security and appropriate use of electronic communication and social media.

4.3 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO), who is the Chief Operating Officer, is responsible for ensuring that identified risks associated with the use of email, the internet and social media are brought to the attention of the Governing Body and are managed appropriately.

4.4 Data Protection Officer

The Data Protection Officer is responsible for the provision of advice on compliance obligations, data protection impact assessment and monitoring of data protection compliance in respect of email, internet and social media use.

4.5 Heads of Service / Line Managers

Heads of Service / line managers are responsible for ensuring their staff are familiar with the content of this policy and procedure and are adequately trained to use electronic and social media safely and effectively.

Heads of Service / line managers are additionally responsible for ensuring that personal use of the internet and email systems by their staff is proportionate, not excessive and does not interfere with their duties.

Requests for internet usage logs must be authorised by an appropriate Head of Service (Appendix B), and such requests should be by exception rather than the norm. The advice of the Human Resources team must be sought and any requests made for internet usage logs must be with the prior agreement of Human Resources.

The Chair of the CCG will undertake the same responsibility for practice representatives on the Governing Body, and the Chief Officer will undertake the same responsibility for all other members of the Governing Body not covered above.

4.6 Staff / Governing Body Members / Associates

Staff/Governing Body members/Associates who are given access to, and responsibility for, using some or all forms of electronic communication and/or social media are responsible for:

- Reading and acting on this policy and procedure
- Seeking advice, assistance and training where required;
  - The CCG's Communications Team should be the first port of call for all social media support and issues. For example; advice and training on how to use social media, and raising any potential concerns in regards to social media posts or content which relate to the work of the CCG. For more information, please see section 5.12 to 5.16.
  - For NHSmail support please visit the online resources at: digital.nhs.uk/services/nhsmail
  - For internet support please contact The Health Informatics Service Desk team by email on: theservicedesk@this.nhs.uk or by telephone on: 0845 127 2600
- Following the guidance in the appendices to this policy and procedure
- Seeking appropriate authorisation from their line managers for blogs, posts and web pages on the CCG's intranet (Skyline) and on the CCG's website, before publication. In addition, staff should also have relevant approval from line managers and the communications team to use CCG social media channels.

5.0 Principles for Using E-communication Tools

The principles set out below apply to online participation, whether for work related or personal use. They set out the standards of behaviour expected from all staff/Governing Body members/associates (including those mentioned in section 1.0) when using any form of electronic communication and/or social media.

Staff should be aware that their line manager has the right to withdraw internet access and/or manage their NHSmail mailbox (to access and read email) if their personal use of the internet (including social media) and email is not in compliance with this policy.

Appendix A of this policy and procedure defines key terms referred to in this section.

5.1 Access to Email and the Internet

The CCG utilises the NHSmail service provided through NHS Digital. All NHSmail accounts are owned by NHS Digital on behalf of the Secretary of State for Health in England.

Access to NHSmail and the internet will be granted along with the network account. To set up a new account, contact The Health Informatics Service Desk on: 0845 1272600. The Application for Network Services form contains

‘Terms of Use’, which must be agreed to in order to use the network, NHSmail and Internet services.

New members of staff joining from an organisation which also uses NHSmail as the primary email account should have already made arrangements as part of the leaver process in their previous organisation for their NHSmail account to have been flagged as a leaver account by the NHSmail Local Organisation Administrator (LOA) in that organisation. On joining, the CCG LOA (The Health Informatics Service) will transfer the NHSmail account to NHS Wakefield CCG.

All staff, governing body members and associates must read and agreed to abide by the NHSmail Acceptable Use Policy before accessing and using NHSmail. If the Acceptable Use Policy is breached or operational requirements dictate, the NHSmail service reserves the right to withdraw access to the NHSmail service without notice.

The NHSmail team reserve the right to update the Acceptable Use Policy as necessary.

Upon leaving the employment of the CCG, it is the line manager’s responsibility to ensure that access to the internet is closed for the member of staff who is leaving the organisation and that their NHSmail account is flagged as a leaver account by the NHSmail LOA.

5.2 Preventing the Spread of Malicious Software (Viruses)

Staff must take all reasonable steps to prevent the receipt and onward sharing by email of malicious software e.g. computer viruses. Staff must keep the computer network safe by:

- Being vigilant for emails from unexpected sources, especially with attachments/links to click on, or emails that appear to be from staff but are written in an unusual style e.g. bad grammar, poor spelling, and excessive use of punctuation
- Not opening unexpected emails or email attachments and making contact with the sender by telephone to verify that the email and its attachment are legitimate
- Ensuring passwords are of a strong password format ie
    - Password must NOT include your username (pre-fix of your email address)
    - Must contain a mix of three out of the following four character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), symbols (!"£$%^&*)
    - Must be 8 or more characters long
    - Cannot be any of your four previous passwords
    - Spaces or commas cannot be used

If staff suspect that a computer or laptop may be infected with a virus or other malware then they should unplug the network cable, turn off the Wi-Fi or shut down the computer immediately and contact The Health Informatics Service

Desk on 0845 1272600 as soon as possible. It is important they do not try to remove the problem themselves or forward any suspicious emails, unless the Service Desk advises this.

5.3 Unacceptable Use of the Internet

The Internet is an important e-communication tool for workplace collaboration. Staff/Governing Body members can additionally use CCG supported devices to access the internet and social media in their own time (i.e. lunchtimes and before/after work).

Internet use by staff/Governing Body members is supported as long as they do **not**:

- Create, deliberately view, download or share (other than for properly authorised and lawful research) any offensive, defamatory, illegal images or data. This includes pornography and discriminatory material. If in doubt, individuals should seek advice from either their line manager or a member of the Information Governance Team
- Create, download or share anything which breaches another person or organisation's copyright. This might include altering software programs, graphics etc. without the express permission of the owner or claiming someone else's work as your own
- Use electronic communication channels to harass individuals or groups in any way
- Deliberately download, upload or share viruses, malware, spam or other malicious data or encourage others to do so
- Bring the CCG in to dis-repute by failing to adhere to the law or your professional staff code of conduct
- Use their position in the CCG to breach patient confidentiality and data. For example; using the internet to search for patient identifiable information.

5.4 Unacceptable Use of E Mail (and Online Messaging)

Although email (and online messaging software such as Skype for Business) may feel less formal than other written communication, the law views it as being exactly the same, so individuals must not:

- Make or share libellous, defamatory, offensive, harassing, discriminatory, obscene or pornographic remarks or images - individuals should take advice from their line manager or a member of the Information Governance Team if they are not sure that they are on the right side of the law
- Share or forward confidential information without permission of the originator
- Send attachments which they know contain a virus or other malware to any other individual
- Forge or attempt to forge messages or send messages using another person's email account

- Send unencrypted emails containing confidential person identifiable information to insecure email accounts. The CCGs NHSmail email accounts are encrypted, and therefore are secure to send/receive personal confidential information. Individuals should ask a member of the Information Governance Team for support if they have any queries about the use of NHSmail for sending or receiving emails containing confidential person identifiable information or other confidential information eg commercially sensitive information.
- Use NHSmail email addresses to register for personal user accounts e.g. eBay, Groupon, personal social networking accounts.

Users of the NHSmail system must comply with the NHSmail Acceptable Use Policy.

5.5 Third Party Access to NHSmail Accounts

All email accounts and email content maintained on NHSmail are the property of the NHS.

The CCG reserves the right to enable third party access to email accounts in exceptional circumstances and without the prior explicit consent of the account holder i.e. to make arrangements to cover long term sickness leave. A request for access form (Appendix C) must be completed as access must be logged and authorised by a Head of Service.

You should have no expectation of privacy for email that you send or receive via the NHSmail service.

5.6 Emailing of Personal Confidential Information and Business Sensitive Information

5.6.1 Using NHSmail to exchange Personal Confidential Information and Business Sensitive Information

As email is generally deemed to be insecure it should not be treated as the standard way of communicating personal confidential information.

No unencrypted personal confidential information should be transferred by email unless there is a legal and justifiable purpose for doing so, appropriate authority, and the sending and receiving email addresses are secure, as described in the following paragraphs.

Where email is agreed as the most appropriate method of transfer for personal confidential information, it may be sent or received using the CCG email system (NHSmail)

NHSmail (.nhs.net) enables the safe and secure exchange of personal confidential information within the NHS and with local/central government.

Between NHSmail addresses:-
.nhs.net to .nhs.net is secure and encrypted

Between NHSmail and Local/Central Government:-
.nhs.net to .gov.uk is secure and encrypted

Between NHSmail and other email accounts:-
.nhs.net to nhs.uk is not guaranteed to be secure and encrypted.

5.6.2 Sending Personal Confidential Information between NHSmail and Local/Central Government

Central Government have retired the secure email service know as Government Connect Secure Exchange (GCSX). This means that councils can no longer send and receive email through their GCSX mailboxes.

You should send and receive person identifiable or sensitive information from your **nhs.net mailbox** to council mailboxes ending in '**.gov.uk'**.

Do not assume that a staff member's name for their '**gov.uk'** mailbox is exactly the same name format as their former GCSX account. Please ensure you confirm the mailbox address before sending email to a new email address.

5.6.3 Sending Personal Confidential Information between NHSmail and other email accounts

NHSmail includes functionality for securely sharing personal confidential information with non '.nhs.net' email accounts (e.g. @any nhs.uk etc.). This involves the recipient signing up to an encryption service to create a secure link between their email and an '.nhs.net' account.

In order to create this link for the first time the NHSmail user must send an email to the insecure address with **[secure]** in the subject field of the email. The word secure is not case-sensitive but it is essential that the word is placed in square brackets (these can be found next to the letter 'P' on a standard keyboard).

When a first encrypted email is received the recipient will be asked to complete a short sign up process to the encryption system. After doing this, the recipient will be able to read and reply to the email securely, as well as securely send and read any attachments.

From this time on, the recipient will be able to securely share personal confidential information with '.nhs.net' email account holders as long as any email containing personal confidential information has **[secure]** in the subject field.

Some non '.nhs.net' email domains in NHS organisations and partner organisations are now secure. For further information on sending and receiving secure emails to non '.nhs.net' email seek advice from the Information Governance Team.

Sending personal confidential information to free email accounts such as the following is prohibited without the explicit permission of the Information Governance Lead:

@yahoo.com @gmail.com @hotmail.com @icloud.com @live.com

5.6.4 Evaluating the Most Appropriate Method of Transfer

Staff should evaluate whether email is the most appropriate method for transferring personal confidential information. Where staff are unsure they should gain approval from their line manager, who should seek advice from the Information Governance Team when necessary.

Factors that will influence whether email is a suitable approach include:

- The type of information
- Its intended use
- Intended frequency of transfer
- The intended recipient(s)
- Availability of common systems for sharing data (e.g. SystmOne)
- The size of the data to be transferred.

Some alternatives to sending personal confidential information via email are:

- Shared network drives.
- THIS SafeDrop - which allows large files or confidential data between different teams and external organisations without relying on email (https://safedrop.this.nhs.uk)
- NHS Digital currently provides alternative file transfer services for specific purposes. These include:
  - Message Exchange for Social care and Health (MESH) https://digital.nhs.uk/services/message-exchange-for-social-care-and-health-mesh
  - Data Landing Platform (DLP) https://digital.nhs.uk/services/data-landing-portal
  - Strategic Data Collection Service Cloud (SDCS Cloud) - successor to SDCS - https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/strategic-data-collection-service-sdcs

If you receive unencrypted insecure personal confidential information from any email address or file transfer service you must report it to the Information Governance Team immediately. It may also be necessary to complete an incident form.

5.6.5 Keeping Personal Confidential Information Safe

- You must never send personal, sensitive or confidential information to a non-secure email address unless it is encrypted.
- Ensure you do not include personal identifiable information in the email subject line field.

- Ensure that any exchange of personal confidential information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated.
- Make sure the information is shared only with the people who are authorised to have it. Emails containing personal confidential information should only be sent to those with a legitimate reason for receiving the information, and only minimal, relevant information should be shared. Caldicott and local information governance principles should apply whenever personal or sensitive information is exchanged.
- Consider whether information being transferred by file attachment could be protected from casual viewing by placing a password on the file being transferred. Speak to your line manager or the Information Governance Team for advice.
- Consider whether the information can be anonymised when sent by email. Anonymised information can be sent using the email system without using any protective measures.
- You must not hold sensitive or personal information in your calendar if your calendar may be accessed by other people. Seek advice from the Information Governance Team if you believe there is a business requirement to hold such information in a calendar.
- Where the email recipient is based outside the United Kingdom, seek advice from the Information Governance Team in the first instance.

5.6.6 Personal Responsibility

All staff are personally responsible for correctly addressing and for sending personal confidential information in a secure manner by email**.**

It is your responsibility to check that you are sending email to the correct recipient, as there may be more than one person with the same name using the NHSmail service. Always check that you have the correct email address for the person you wish to send to – this can be done by checking their entry in the NHS Directory.

It is your responsibility to ensure your details in the NHS Directory are correct and up to date.

5.7 Emailing Service Users

Email can be an efficient communication method between staff and service users. The form in Appendix E should be used before communicating sensitive personal information with service users by email, where service users have made a specific request to communicate via this method.

The risks associated with emailing service users include but are not limited to:

- Email to public internet email address (e.g. Jane@googlemail.com) is not secure at any point
- A virus could spread personal and sensitive email to other computers

- If an attachment is used then a ‘cached’ copy of the correspondence will reside on the computer that the email is opened on (the service user) and may be able to be accessed by others who have access to their computer.

5.8 NHSmail and Home / Remote Working Responsibilities

NHSmail may be used outside the NHS network on any computer with an internet connection, via a web based interface. However you are personally responsible for the information security and confidentiality of e-mail in your NHSmail account and must observe the following conditions when accessing NHSmail at home or other remote locations outside the NHS:-

- Log in at the NHSmail website: www.nhs.net
- **If using a non CCG organisation device you must ensure** the “This is a Private Computer” tick box option is **unticked.** This will enable you to safely view file attachments without them downloading to the computer device hard drive.
- Be aware that if you tick “This is a Private Computer” when logging in, this will enable file attachments to be downloaded to the computer and could put you and the organisation at risk. **Do not** download any confidential or other work related information to a non-organisation device.
- Only print confidential information when you are certain that you will always collect the printouts immediately and secure them
- Ensure that you are not overlooked by family members and others with no right to see the information
- Do not record your password on a non-organisation device
- Log out of the NHSmail application when not in use
- Do not leave the NHSmail application logged in when unattended.

If you believe you have a specific requirement to work from home, please talk with your line manager in the first instance.

5.9 NHSmail and Use of Mobile Devices

Mobile phones, handsets or tablets that can be used to make phone calls, will have the technical ability to connect to NHSmail. In the context of this policy, a laptop computer is not defined as a mobile device.

You **must** obtain approval from the CCG to use a personal device with NHSmail to ensure you comply with local information governance requirements and NHS policy on encryption. Please speak to the Information Governance Lead in the first instance.

5.10 Email Best Practice

A well written and structured email helps to enhance and improve image and reputation (both at an individual and organisational level). Staff are encouraged to follow the best practice guidelines below:

- ✓ Include your name, job title and contact number(s)
- ✓ Use the spell checker!

- ✓ If you need a reply to your email by a particular date, say so
- ✓ Only mark emails as important if they really are important
- ✓ Check that you have addressed the email to the correct recipient(s) and/or distribution list. Take care when using the ‘auto complete’ feature to address emails as it can be easy to address the email to the wrong recipient(s)
- ✓ Don’t clutter inboxes - use to: and cc: wisely, ask yourself if that person really needs to see the email?
- ✓ Answer emails as quickly as possible
- ✓ Think before using ‘Reply to all’. Only use ‘Reply to all’ if you really need your message to be seen by each person who received the original message.
- ✓ Only print emails if you really need to for work purposes
- ✓ Use your ‘out of office’ when you know you won’t be picking up messages for a while. Give your return date and an appropriate individual’s name/number as a contact for anything urgent
- ✓ Don’t use your mailbox as an electronic filing cabinet. Manage your mailbox and delete any sent/received messages you don’t need to retain and empty your ‘deleted items’ folder regularly
- ✓ Where you identify emails which need to be retained in line with minimum record retention periods, these must be saved within the relevant corporate filing system (paper or electronic) and deleted from your mailbox. For further information please refer to the section called ’Emails as Records’ on page 17 of the Records Management and Information Lifecycle Policy. If you are unsure how to save emails to the shared drive area, seek advice from Skyline or your line manager. When moving your NHSmail account between health and care organisations, it is your responsibility to ensure any data relating to your role is archived appropriately and is not transferred to your new employing organisation in error.
- ✓ Be aware that emails save in the ‘Deleted Items’ folder are classed as being reasonably accessible for the purposes of searches for information under the Freedom of Information Act.

5.11 Text Messaging and WhatsApp

Text messaging and the use of WhatsApp are becoming more common in the NHS, in particular for use in crisis communications.

There are, however, some important data protection considerations surrounding the use of these systems, including:

- The transfer of sensitive data across unregulated servers outside the European Economic Area (EEA)
- Compliance with data protection requirements regarding ‘fair processing’, individuals’ rights, and records management
- Data protection security risks, including using your own device for work purposes.

A proportionate approach is therefore needed: staff need to balance the benefits and risks of instant messaging depending on the purpose for which they wish to use it (e.g. using it in an emergency versus as a general communication tool). Staff should also remember that work related communication sent and received via these ‘media’ are also subject to Freedom of Information and data protection law.

Below are key guidelines which **must** be adhered to, should staff, Governing Body members and CCG associates need to communicate via text or WhatsApp:

- Please speak to your line manager should you require a work mobile phone to complete your work related duties.
- The security features of an app can help ensure that your message stays private between you and the intended recipient or recipients. WhatsApp has end-to-end encryption (AES 256) and therefore would be suggested as the primary messaging application
- Do not use patient identifiable data when communicating via text messaging or WhatsApp
- Remember that instant messaging conversations may be subject to disclosure laws such as freedom of information and data protection – as such, be professional in your tone and be careful with personal comments and opinions
- Text and WhatsApp messages should be kept and recorded appropriately in line with any record management responsibilities e.g.- due to a major incident. Where you identify messages and content (transcribed if required) which need to be retained, these should be saved for the minimum required retention time in the relevant filing system on the shared drive or relevant paper record. For further information please refer to the section called ’Emails as Records’ on page 17 of the Records Management and Information Lifecycle Policy
- Keep your device secure and in sight:
    - Don’t allow anyone else to use your device
    - Set your device to require a passcode immediately, and for it to lock out after a short period of not being used
    - Disable message notifications on your device’s lock-screen
    - Enable the remote-wipe feature in case your device is lost or stolen.
- The following particular care should be taken when using WhatsApp primarily:
    - Ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device’s address book
    - If you are an instant messaging group administrator, take great care when selecting the membership of the group, and review the membership regularly
    - Switch on additional security settings such as two-step verification
    - Review any links to other apps that may be included with the instant messaging software and consider whether they are best switched off
    - Separate your social groups on instant messaging from any groups that share clinical or operational information
- Unlink the app from your photo library.

5.12 Unacceptable Use of Social Media

Social media means web-based tools which allow users to communicate with each other across the worldwide web. This includes blogs, message boards, social networking and content sharing websites such as Facebook, Twitter, LinkedIn, Instagram, WhatsApp, YouTube. Social media allows peer to peer communication and development of new ‘virtual’ communities.

Social media is a platform which will allow the CCG 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.

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 a member of staff 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, remember that the information you give about yourself may link you to the organisation and leave your comments open to being interpreted as the views of the organisation. When using social media:

- 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
- Be aware that online comments are usually permanent; they can be republished in other media and that anything said may attract media interest
- Remember that all staff are ambassadors for NHS Wakefield CCG
- Be responsible and honest at all times
- Share any learning or information gathered via social media with others where appropriate
- Be credible, accurate and fair
- Never give out personal details such as home address and private phone numbers
- Take advice from a senior manager and/or the communications team if in doubt
- Stay within the law and be aware that libel, defamation, intellectual property law (patents, trademarks and copyright) and data protection laws apply

- Do not use your position at the CCG to breach patient confidentiality and data. For example; using social media to search for patient identifiable information
- Do not post defamatory, derogatory or offensive comments on the internet about staff, patients, their work or the CCG
- Do not reveal or use any confidential or personal information about patients, or staff.

Individuals whose use of social media brings themselves, the CCG or staff into disrepute may be subject to disciplinary action in line with the CCG's Disciplinary Policy.

Before beginning to use a social media channel, consider:

- What other channels could be used to reach the intended audience
- The level of resource needed to maintain and monitor some social media sites – they need to be kept 'alive' via new content and messages.

5.13 Guidelines for Using Social Media

Staff/Governing Body members/ associates must take the following into consideration when using social media:

- ✓ Know and follow NHS Wakefield CCG's Electronic Communication and Social Media Policy and Procedure, along with associated policies and procedures (set out in Section 10)
- ✓ Understand your responsibilities to stay within the law and not bring your employer into disrepute.
- ✓ Respect intellectual property (copyright, patents and trademarks), fair use and financial disclosure laws
- ✓ Ask and seek permission to publish or report on conversations that are meant to be private or internal to NHS Wakefield CCG. Don't cite or reference staff, services or organisations without their approval. When you do make a reference, where possible link back to the source
- ✓ Do not post any patient identifiable information, including photographs of members of the public without explicit consent
- ✓ Respect your audience. Don't use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory—such as politics and religion
- ✓ Be aware of your association with NHS Wakefield CCG and other NHS organisations in online spaces. If you identify yourself as an NHS Wakefield CCG / NHS staff member, ensure your profile and related content is consistent with how you wish to present yourself with staff and the general public
- ✓ Do not pick fights, be the first to correct your own mistakes
- ✓ Do not alter previous posts without indicating that you have done so
- ✓ Try to add value. Provide worthwhile information and perspective. The NHS brand is well respected and enhanced by its people. What you publish may reflect on NHS Wakefield CCG's reputation or the NHS as a whole.

Please read Appendix G for more social media guidance.

5.14 Setting up a Corporate Social Media Account

CCG staff are not permitted to set up “business use” groups, blogs or any other form of social media which is NHS Wakefield CCG branded or contains content for which NHS Wakefield CCG owns the copyright. In addition, patient information is forbidden to be shared on such groups.

The CCG has a number of social media channels which are monitored and managed by the central Communications Team. These include:

Twitter

- @NHSWakfieldCCG
- @NHSVanguardWake

Facebook

- @HealthyWakefield

NHS Wakefield CCG asks that staff/Governing Body members utilise the CCG’s established social media channels and contact the CCG’s Communications Team to discuss any relevant information to be shared on social media.

Organisations hosted by the CCG are viewed as separate entities and are able to create and host their own, organisational-branded social media accounts. However, these host organisations must act within the constraints of this Policy and be responsible for the content of their own accounts.

For more information, please speak to the CCG’s Communications Team.

5.15 Social Media Support, Training and Advice

The CCG’s Communications Team are able to provide support and advice in regards to social media usage and management.

Contact the team on WAKCCG.Press.Office@nhs.net for further support.

5.16 Reporting a Social Media Incident

Please follow the Incident Reporting Policy should an incident on social media occur. If you are unsure as to whether a potential incident requires reporting, please contact the CCG’s Information Governance team for advice.

6.0 Monitoring Usage

6.1 Email

All emails including personal emails are monitored for viruses and to maintain the size of accounts. All email traffic (incoming and outgoing) is logged.

These logs are audited periodically. The content of emails is not routinely monitored.

The CCG reserves the right to inspect, monitor and retain message content. In exceptional circumstances this may be without the prior explicit consent of the staff member (only to the extent that it will not contradict relevant clauses in the Human Rights Act) as required to meet legal, statutory and business obligations. See Section 5.5 for 3rd party access process.

6.2 Internet

Staff should be aware that when they visit a website for work or personal use that information is recorded as part of an automated monitoring process. This includes details of websites visited, duration of visits and downloaded files. Staff should be aware that this monitoring may reveal sensitive data about them, if they use CCG internet access facilities for personal use.

For example visits to websites of a particular political party or self-help advice sites may indicate your political opinion or identify a physical or mental health condition. By making use of the CCG internet access facilities, staff are consenting to the CCG processing any sensitive person data about them, which may be revealed through monitoring.

Staff who do not consent must take responsibility for the maintenance of their own personal privacy by not using the CCG systems to access this type of information.

The CCG has implemented technical measures to actively block access to websites which are deemed “inappropriate”, e.g. pornographic or otherwise offensive websites (details at Appendix D). If a legitimate purpose exists, necessitating access to websites categorised as “inappropriate”, staff should speak with their line manager to establish the purpose and authorise the request for access. The Service Desk retains the facility to ‘unblock’ access under such circumstances.

Information recorded by the automated monitoring systems can be used to identify an individual user and show, for example, a website or document that a user has been viewing and the time spent browsing. Because of this, staff must not assume privacy in their use of CCG’s systems, even when accessing the systems in their personal time i.e. out of paid working hours.

On behalf of the CCG, The Health Informatics Service will undertake regular reviews of the internet activity logs to monitor IT system performance.
The Health Informatics Service will undertake reviews at the specific request of the CCG Information Governance Lead (in collaboration with the Human Resources representative). This may include review of usage and investigation of incidents and will be managed in accordance with local CCG procedures.

The CCG also reserves the right to carry out detailed inspection of any IT equipment without notice, where inappropriate activity is suspected.

Any inappropriate use of the internet detected, either incidentally during routine monitoring or through audit activities, will be reported to the relevant CCG senior manager (or nominated deputy), who will be responsible for coordinating an appropriate and proportional response and, where appropriate, instigate action under the CCG Disciplinary Policy and Procedure.

Managers with concerns should refer to their Human Resources representative, who will in turn contact the CCG Information Governance Lead in respect of any investigation to be conducted.

If evidence exists that indicates any users are failing to adhere to this policy and procedure or are using the Internet in an inappropriate manner the CCG reserves the right to investigate Internet usage under these circumstances. The CCG also reserves the right to take disciplinary action; this will be dealt with under the CCG Disciplinary Policy and Procedure.

7.0 Implementation and Dissemination

Following ratification by the Integrated Governance Committee this policy and procedure will be disseminated to staff/Governing Body members via the CCG's intranet and in-house communication mechanisms.

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

8.0 Monitoring Compliance with and Effectiveness of the Policy

To be assured that this policy is being implemented, key elements will be monitored for compliance, including:

- All staff receive annual training and competency test in Data Security Awareness Level 1. The Integrated Governance Committee will monitor progress via the workforce update report
- Number of disciplinary issues relating to the use of email, the internet and social media. The Integrated Governance Team will monitor progress via the workforce update report.

9.0 References

www.getsafeonline.org

10.0 Associated Documentation (Policies, protocols and procedures)

The CCG has a suite of information governance and supporting policies including:

- Information Governance Policy and Framework
- Information Security Policy (incorporating Network Security)
- Confidentiality and Data Protection Policy

- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Equality & Diversity Policy
- Acceptable Standards of Behaviour Policy
- Disciplinary Policy and Procedure
- Media Handling policy
- NHSmail Acceptable Use Policy. A copy of the current version can be found at https://digital.nhs.uk/services/nhsmail/nhsmail-policies

And their associated procedures (including but not limited to)

- Access to Records Procedure
- Data Protection Impact Assessment and Information Governance
- Checklist processes
- Safe Haven Guidelines and Procedure
- Confidentiality Audit Procedures

This policy and procedure should be read in conjunction with the above policies and procedures as well as the Information Governance User Handbook which has been shared with all staff and for which new staff will need to sign for receipt and confirm that they have read the document.

11.0 Equality Impact Assessment

The CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

Attached at Appendix F Equality Impact Assessment.

Definitions

1.1 Defamation and Libel

What is defamation and libel?

A published (spoken or written) statement or series of statements, which affects the reputation of a person or an organisation and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law.

DO NOT

Make statements about people or organisations on any web pages you are including on the website or in any email that you write without verifying their basis in fact.

1.2 Harassment

What is harassment?

Any unwarranted behaviour, which is unreasonable, unwelcome or offensive. This may include physical contact, comments or printed material, which causes the recipient to feel threatened, humiliated or patronised.

Harassment takes many forms. It can range from extreme forms such as violence and bullying, to less obvious actions like ignoring someone at work. Whatever the form, it will be unwanted behaviour that is perceived as unwelcome and unpleasant by the recipient. Harassment can be on a variety of grounds, including sex/gender, race, sexual orientation, religious beliefs, age, physical/mental disability. Note that this list is not exhaustive.

DO NOT

Use the internet to harass other members of staff by displaying particular websites that they consider offensive or threatening or using email to harass other members of staff by sending messages that they consider offensive or threatening.

1.3 Pornography

What is pornography?

Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography that is legal in the UK may be considered illegal elsewhere. Because of the global nature of Internet these issues must be taken into consideration. Therefore, the CCG defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The CCG will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

DO NOT

- Create, download, save or transmit pornography
- Send, deliberately view or forward emails with attachments containing pornography. If you receive an email with an attachment containing pornography you should report it to your line manager and the Service Desk, as soon as possible.

Indecent Images of Children – Guidance for Managers

It is a criminal act under Section 1 of the Protection of Children's Act 1978 for any person to make and distribute indecent images of children. These are arrestable offences.

Upon receipt of any information concerning this kind of activity, the Head of Service should notify the Police (Child and Public Protection Unit) immediately and advise the Information Governance Lead along with the relevant Human Resources representative. No downloading or distribution of any images should be completed, either internally or externally within the organisation, as this may leave the individual(s) responsible open to criminal investigation.

The computer should be left and not used by anyone, allowing this to be seized as evidence for forensic examination by the Police. The details of all persons having access to the computer should be made available to allow a clear evidence trail to be established.

What are the consequences of not following this policy?

- Users and/or the CCG can be prosecuted or held liable for transmitting or downloading pornographic material, in the UK and elsewhere
- The reputation of the CCG will be seriously questioned if its systems have been used to access or transmit pornographic material and this becomes publicly known
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, will be dealt with under the CCG Disciplinary Policy and Procedure
- This may constitute gross misconduct under the CCG Disciplinary Policy and Procedure.

1.4 Copyright

What is copyright?

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright. In the case of CCG standard use computer software, the CCG purchases licences on behalf of its users.

DO NOT

- Alter any software programs, graphics etc. without the express permission of the owner
- Claim someone else’s work is your own
- Send copyrighted material by Internet without the permission of the owner. This is considered copying.

1.5 Computer Misuse Act 1990

Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other User’s data or hardware is an offence under the Computer Misuse Act 1990.

2. FURTHER INFORMATION

If you would like any further information please contact the Information Governance Team: IGSharedService@calderdaleccg.nhs.uk

APPENDIX B

Request for access to the internet usage logs

I request that the Information Governance Team of The Health Informatics Service carry out a search of the internet usage logs for:

Name of user: ……………………………...…………

Job Title / Role:…………………………………………....

Location:……………………...…………………

Dates to be searched: ………………………………………...

I believe that this individual has been accessing inappropriate material on websites contrary to NHS Wakefield CCG's Electronic Communication & Social Media Policy and Procedure.*

I believe that this individual has been using the internet for excessive personal use contrary to NHS Wakefield CCG's Electronic Communication & Social Media Policy and Procedure.*

* Delete as appropriate.

Signed …………………………………………….

Date………………………………………………...

Name………………………………………………..

Position…………………………………………….. Head of Service

APPENDIX C

Request for access to a user’s NHSmail account where permission has not, or cannot be obtained from that user

I request that the Service Desk of The Health Informatics Service grant access to the following user’s NHSmail account:

Name of person to access account ………………………………………….

Job Title: …………………………………………....

Location: ……………………...…………………

Name of user’s account to be accessed: …………………………….……

Job Title: …………………………………………....

Location: ……………………...………………..…

The user named above is on - unplanned absence / left NHS Wakefield CCG / other

(Please specify)……………………………………………*

Or

I believe that the user has been using the email system contrary to the NHS

Wakefield CCG e-Communication and Social Media Policy and Procedure and/or NHSmail Acceptable Use Policy.*

* Delete as appropriate.

An appropriate ‘Out of Office’ message must be placed on the account, when

applicable. An Auto forward rule must be placed on the account.

Signed ……………………………………………. Date…………………

Name………………………………………………..

Position…………………………………………….. Head of Service

Internet Content Filtering

The CCG has implemented technical measures to actively block access to websites which are deemed “inappropriate”, e.g. pornographic or otherwise offensive websites.

The following categories of website are currently being blocked.

- Adult / Sexual Activity
- Criminal Activity
- Gambling
- Hacking
- Intolerance / Hate
- Phishing / Fraud
- Proxies
- Spam
- Spyware
- Tasteless
- Violence
- Weapons

Users are warned about accessing the following categories of websites

- Illegal Drugs
- Intimate Clothing & Swimwear
- Ringtones

All Internet traffic is logged automatically. Monitoring software is in use for back-up purposes and to protect the security and integrity of CCG systems.

Any inappropriate use of the internet detected, either incidentally during routine monitoring or through audit activities, will be reported to the relevant Head of Service, who will be responsible for co-ordinating an appropriate and proportional response and, if necessary, instigating action under CCG’s Disciplinary Policy and Procedure.

If you would like any further information about internet filtering please contact the Health Informatics Service Desk Telephone: 0845 127 2600 Email - theservicedesk@this.nhs.uk

APPENDIX E

Request to Correspond via Personal Email Address

NHS Wakefield CCG recognises that with advancing technology, current and routine forms of communication may not be convenient or possible for you to use to correspond with the CCG.

Where you have made a specific request, verbally or in writing, to correspond with the CCG by email we are willing to communicate via email with you under the following conditions:

- On the understanding that the CCG has no responsibility for information that leaves authorised NHS networks at your request and as such we cannot guarantee the security of such information
- On the understanding that the CCG has no responsibility for equipment personally used by yourself
- You will tell us as soon as possible if your email address changes
- You have satisfied yourself that access to your own system is secure and you are aware of the risks of shared email accounts, shared computers etc.

To minimise the risk of ‘human error’ in addressing new emails, you agree to send an initial email to a representative of the CCG. This will provide us with your preferred email contact address and will be used by us to correspond with you.

We reserve the right to terminate this agreement if there is any virus or other such technical threats to our internal systems as a result of external email traffic.

By signing below you are indicating that you have read and understood the conditions given above and understand that you are able to review or cancel this arrangement at any time in writing.

Your Name ……………………………………………………………

Your Address …………………………………………………………

Your Signature…………………………………………………………..

Agreed on behalf of NHS Wakefield CCG ……………………………………….

Signature ………………………………………………………….

Print Name…………………………………………………………

APPENDIX F

Equality Impact Assessment

Title of policy	Electronic Communication and Social Media Policy and Procedure
Names and roles of people completing the assessment	Information Governance Manager
Date assessment started/completed	6th May 2019

1. Outline	
Give a brief summary of the policy	The purpose of the policy and procedure is to ensure all staff and Governing Body members understand the principles for using email, the internet and social media in lawful and responsible way. Additionally, the purpose is to give best practice guidance on using e-communication tools safely and effectively at work and at home.
What outcomes do you want to achieve	The outcome from effective implementation of the policy should be that everyone connected with NHS Wakefield CCG uses electronic communication and social media at work (and at home) in a way that protects the CCG and themselves from legal consequences including breach of confidentiality, cyber-crime and reputational damage

2.Analysis of impact			
This is the core of the assessment, using the information above detail the actual or likely impact on protected groups, with consideration of the general duty to; eliminate unlawful discrimination; advance equality of opportunity; foster good relations			
	Are there any likely impacts? **Are any groups going to be affected differently?** **Please describe.**	**Are these negative or positive?**	**What action will be taken to address any negative impacts or enhance positive ones?**
Age	No	Neutral	There is some evidence of some social media platforms varies according to the age of staff/service users.
Carers	No	Neutral	
Disability	No	Neutral	There is some evidence that use of email/Internet/social media may benefit some people with a disability; or they may be excluded, depending on whether they have access to email/Internet/social media and have assistive technology that is compatible.
Sex	No	Neutral	
Race	No	Neutral	If posts are in English only, this may impact negatively on people whose first language is English
Religion or belief	No	Neutral	
Sexual orientation	No	Neutral	

Gender reassignment	No	Neutral	
Pregnancy and maternity	No	Neutral	There is some evidence that use of email/Internet/social media may benefit staff on maternity leave, providing they have access to email/Internet/social media.
Marriage and civil partnership	No	Neutral	
Other relevant group	No	Neutral	Use of email, Internet and social media may be: • Of benefit to some groups with protected characteristics listed above, plus part-time or remote workers • Inaccessible to some groups e.g. people who do not use email or the Internet, do not have compatible technology/hardware. However, any potential negative impacts associated with email/Internet/Social Media use are mitigated as these are not the only form of communication with staff or service users. This policy promotes good practice and includes safeguards to prevent people from

			protected groups from discrimination, harassment and victimisation.
Human Rights	Yes	Potentially negative in relation to accessing of emails and internet usage.	Monitoring of email and internet usage must ensure that the employee’s right to privacy is respected. However, in exceptional circumstances and following proper protocol, individual’s privacy cannot be guaranteed at work.
Health Inequalities	No	Neutral	

If any negative/positive impacts were identified are they valid, legal and/or justifiable? **Please detail.**	No anticipated detrimental impact on any equality group. This policy is applicable to all staff and adheres to legal requirements and best practice. There are no statements, conditions or requirements that disadvantage any particular group of people with a protected characteristic.

4. Monitoring, Review and Publication			
How will you review/monitor the impact and effectiveness of your actions	Monitoring of any issues of harassment and discrimination of protected groups of staff (or other) relating to the use of email, the internet and social media.		
Lead Officer	**Governance and Board Secretary**	**Review date:**	**April 2020**

5.Sign off			
Lead Officer	Sarah Mackenzie-Cooper, Equality and Diversity Manager		
Director	Director of Corporate Affairs	**Date approved:**	May 2019

APPENDIX G

Social media guidance for staff

Introduction

Social media is fun - lots of us already use it to stay up to date with news or keep in touch with friends and family. Social media is also powerful - increasingly people are finding it has huge potential for professional networking and development.

Ultimately, social media is about conversations and we no more want to tell you exactly what to say on Facebook or Twitter than we want to tell you exactly what to say on the phone or in emails. But just like on the phone or in emails, there are good habits and practices, things to be mindful of, and behaviours to completely avoid.

We really want people to get the most out of social media, while avoiding some of the pitfalls that this method of communication can present. Whether you use social media personally, professionally or both, these guidelines aim to help you approach it in a way that will protect and enhance both your own reputation and if applicable, the reputation of your organisation.

The purpose of this guidance is to ensure you are aware of the proper, effective and lawful use of social media. This can be as a member of staff who uses social media as part of their job or who uses it in a personal capacity that may have an impact or effect on people using our services, our organisations, staff, contractors or partner organisations.

The guidance builds on work undertaken by health and social care organisations in Leeds.

Using social media

As with any form of communication, we should all be using our common sense when using social media. So what should and shouldn't you do? These are the important points:

Privacy settings – understand and check your privacy settings on your social media profiles. You may also wish to consider how much personal information you include on your profile.

Be professional - when posting, assume your comments are public for all the world to see. If you are representing your profession or organisation you should be polite, open and respectful. Make sure that what is said online is consistent with other communications. Try to avoid getting angry or taking comments personally. It can sometimes be helpful to take difficult conversations offline. Staff should remember they may not have disclosed their association with the CCG but their association may be public knowledge anyway. When using social media these staff should assume that their disclosures will be associated with the CCG.

Confidentiality – in all cases, confidentiality must be respected. Do not post information which could lead to the identification of someone using your service, or a staff member, without their permission. This could breach their right to confidentiality and you could breach your Professional Code of Conduct. Do not disclose personal or business sensitive (protectively marked) information about your organisation, its staff, customers or any other stakeholders.

Only share content that you are happy to be public knowledge - all postings to social media websites should be considered in the public domain. Therefore, only post comments, videos and pictures which you would be happy to share with any group of friends or strangers. Don't post photographs of people without their permission or use images without consent. Remember once you have published information you cannot guarantee it can be fully removed, and you cannot control how it is shared.

Be transparent - any accounts or profiles which relate to your organisation should be clearly and easily identified as such and should have approval. Branding and logos - only use your organisation's logo or branding if you are authorised to speak on behalf of the organisation.

Be responsive – if responding to questions or comments on behalf of a service or organisation, do so in a timely and informative manner and remember that expectations for response times are more immediate for social media.

At work - only use social networking sites at work for work purposes. If in doubt, speak to your line manager about whether using social media for your work is appropriate.

Accepting friend requests or similar - for staff who directly provide care or support, you should not accept friend requests on Facebook and on Twitter do not follow or respond to @mentions from people who you are directly caring for. The same principle applies to other social networks such as LinkedIn or Google+. You may wish to have a conversation about your organisation's social media guidelines with people you support. And remember: do not respond to requests for clinical advice on social media.

Conduct

Your organisation's code of conduct applies online as it does anywhere else and should be adhered to on social media. Not following this guidance may be regarded as serious and could result in disciplinary action. For further information please contact the CCG's Communications Team.