NHS
Vale of York
Clinical Commissioning Group

INTERNET, EMAIL AND ACCEPTABLE USE POLICY

November 2018

Original Authorship :	Information Governance Security and Compliance Manager, North Yorkshire and Humber Commissioning Support Unit
Reviewing Committee :	Governance Committee
Date :	22 November 2018
Approval Body :	Executive Committee
Approved Date :	20 March 2019
Review Date :	November 2020
Equality Impact Assessment :	Yes
Sustainability Impact Assessment :	Yes
Related Policies	• IG02 Data Protection and Confidentiality Policy • IG04 Freedom of Information Policy • IG05 Information Security Policy • IG06 Information Risk Policy • IG07 Corporate Records Management Standards and Procedures • IG08 Mobile Working Policy • IG09 Subject Access Request Policy • IG10 Safe Haven Policy • IG11 Information Governance Strategy
Target Audience :	All Staff
Policy Reference No. :	IG03
Version Number :	4

POLICY AMENDMENTS

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

New Version Number	Issued by	Nature of Amendment	Approved by and Date	Date on Internet
0.1	Barry Jackson	Small amendments	NR	
1.0	P. Furneaux, Vale of York CCG	Amendments: Policy Merger of Acceptable Computer Use Standard and Email Standard. CCG specific amendments. Inclusion of: Additional guidance from NHSMail standards and guidance regarding synchronisation of devices, iCloud storage etc. Social Media Policy	Management Team 05 March 2014	
2.0	M. Skelton Vale of York CCG	Addition of Responsibilities re Lost and Stolen Devices	SMT February 2016	
3.0	M. Hughes Vale of York CCG	Updated the procedure for the removal of NHS mail from phones. Amended name of CCG support to eMBED. Added in Introduction, policy statement, scope, policy purpose, policy implementation, training and awareness, monitoring and audit, policy review, references, associated policies and contact details. Reference to the General Data Protection Regulation Use of non CCG devices or systems as follows: • Plugging in personal equipment into a work device • Accessing Non-work related third party applications from work devices • Accessing personal	Exec Committee 15 November 2017	15 January 2018

		email systems or personal social media accounts from work devices Change to guidance on use of secure email (NHSMail)		
3.1	IG Specialist	Updates to Data Protection Act 2018 Addition of Appendix 3 – The CCG's Social Media Accounts	Goverane Committee 29 Jan 2019 CCG Exec. 20 March 2019	29 March 2019

To request this document in a different language or in a different format, please contact the CCG :

01904 555870 or valeofyork.contactus@nhs.net

NHS
Vale of York
Clinical Commissioning Group

Contents

1 INTRODUCTION

1.1 Internet and email is an important part of the CCG's and the wider NHS communications system. Use of the installed systems/connections is for legitimate work related purposes only and is encouraged to improve the quality of work and productivity in patient care, research, operational matters, education and development.

1.2 We must, however, ensure that the increasing use of information technology maintains patient confidentiality, is not misused, and at the same time is secure and accurate. This policy provides guidance on the CCG's expectations for the use of the internet and email.

2 POLICY STATEMENT

2.1 The purpose of this document is to present a policy for the acceptable use of the internet and email. This sets out the expectations of the CCG for the proper use of its email systems and compliments other Information Governance policies. Its aim is to ensure the appropriate and effective use of the internet and email by :

- Setting out the rules governing the sending, receiving and storing of email
- Establishing user rights and responsibilities for the use of systems
- Promoting adherence to current legal requirements and NHS information governance standards

2.2 This policy is applicable to all employees, agents and contractors working for, or supplying services to the organisation. However, it is recognised that primary care practitioners are also part of the organisations and as such this policy is offered for use by them to adapt to their own practices and organisations as appropriate. The contact for the policy is available to offer help and support.

3 IMPACT ANALYSES

Equality

3.1 As a result of performing the screening analysis, the policy does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage. The results of the screening are attached.

Sustainability

3.2 A Sustainability Impact Assessment has been undertaken. No positive or negative impacts were identified against the twelve sustainability themes. The results of the assessment are attached.

Bribery Act 2010

3.3 The Bribery Act is particularly relevant to this policy. Under the Bribery Act it is a criminal offence to :

3.3.1 Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and

3.3.2 Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.

3.3.3 These offences can be committed directly or by and through a third person and other related policies and documentation (as detailed on the CCG intranet) when considering whether to offer or accept gifts and hospitality and/or other incentives.

3.3.4 Anyone with concerns or reasonably held suspicions about potentially fraudulent activity or practice should refer to the Local Anti-Fraud and Corruption Policy and contact the Local Counter Fraud Specialist.

4 SCOPE

4.1 This policy applies to all CCG employees, Council of Representatives, Members of the Governing Body, members of its committees and sub-committees, Lay Members, any staff seconded to the CCG and contract and agency staff. Any reference to staff or individuals applies to all the aforementioned.

4.2 This policy covers all staff employed by the CCG while they are at work either within CCG premises or at any other location in pursuance of their normal work activities.

4.3 Staff working in CCG premises who are not CCG employees must follow the policy of their employer, however the results of risk assessments carried out in CCG premises that they work in must be shared with them and their risk assessments shared with CCG staff.

5 POLICY PURPOSE / AIMS AND FAILURE TO COMPLY

5.1 The CCG's Email and Internet Acceptable Use policy is designed to help you understand the CCG's expectations for the use of the Internet and/or email.

5.2 All existing policies and procedures apply to your conduct on the Internet and whilst using the email system, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of CCG resources, harassment, information and data security, and confidentiality.

5.3 Failure to comply with the requirements of this policy, including non-compliance with the Computer Misuse Act 1990 and current Data Protection Legislation, or infringement of copyright, will be regarded as serious misconduct which will result in disciplinary action being taken. Although each case will be judged on its own merits, misuse of the Internet/Email (or any misuse of computer systems) may be considered Gross Misconduct and will lead to disciplinary action which may result in dismissal.

6 ROLES / RESPONSIBILITIES / DUTIES

6.1 Email introduction

6.1.1 The Vale of York Clinical Commissioning Group (the CCG) has adopted the national NHS Mail system as its e-mail solution for all staff. Staff must ensure that they follow the NHS Mail Policies available through the Health and Social Care Information Centre website http://systems.hscic.gov.uk/nhsmail in conjunction with local policies and procedures.

6.1.2 Applicability. All staff employed by the CCG will have access to an NHS mail account. Contractors and temporary staff may also be granted accounts where appropriate. All CCG official business must be conducted on NHS Mail accounts. Non NHS Mail accounts are not permitted in any formal Distribution Lists without the approval of the Head of Governance.

6.1.3 Security. NHS Mail is a secure system operated for the NHS which is approved for the sending of patient level data. It is government accredited to RESTRICTED status and approved for exchanging clinical information with other NHS Mail accounts and Government Secure intranet (GSi) users by the Department of Health and endorsed by the British Medical Association, Royal College of Nursing and Chartered Society of Physiotherapy. GSi domains that are secure for the exchange of patient data are : .x.gsi.gov.uk; .gsi.gov.uk; .gse.gov.uk; .gsx.gov.uk; .pnn.police.uk; .cjsm.net; .scn.gov.uk; .gcsx.gov.uk, .mod.uk.

6.1.4 Virus Protection. IMT will ensure that the appropriate technical steps are taken to reduce the vulnerability of the eMBED systems to attack from computer viruses. Users are expected to play their part by being aware of the problem of viruses and reporting anything they deem to be suspicious to the IT Helpdesk. Users should note in particular to be very wary of e-mails from addresses that they do not recognise and under no circumstances open an attachment on an e-mail if it is not from a recognised address.

6.1.5 Monitoring. Staff are advised that in accordance with the Employment Practices Data Protection Code monitoring of E-mail traffic will take place subject to the following guidance :

- Monitoring is required to ensure that employees do not breach any regulations (such as those on harassment) which could have a legal impact on eMBED.
- The Information Governance Team, on the specific authorisation of the Head of IMT, will carry out checks.
- Spot checks will be done as opposed to continuous monitoring.
- Traffic will be monitored as opposed to content unless there are reasons for checking specific e-mails.
- emails that are obviously personal will not be opened without the individuals consent.
- Inappropriate use of the e-mail may result in the facility being withdrawn and may constitute an offence under the NHS disciplinary code.

6.1.6 Bandwidth. This is the term that is used to describe the amount of information that can be transmitted on a network over a given time. Individual users sending very large files such as videos or sending to large numbers of addressees can have an adverse effect on the availability of the network for other users. To avoid this users should be aware of the problem and where possible avoid sending large e-mails with attachments. Text should be included in the body of the message as opposed to attaching a Word document, and where a file can be located on the network or Intranet the location should be given rather than copying the file. This is particularly important for multiple addressees.

6.1.7 eMBED

eMBED manages NHSMail services on behalf of the CCG. Line managers are responsible for informing the eMBED of starters and leavers to enable eMBED Local Organisation Administrators (LOAs) to appropriately manage user access to N3 hosted email services. eMBED will also ensure that local arrangements are in place to manage compliance with HSCIC NHSMail policies and procedures on behalf of the CCG in line with agreed SLA arrangements.

6.2 Access

6.2.1 Email accounts can be accessed in the following ways :

- Organisation PC or laptop using Microsoft Outlook.
- Organisation PC or laptop using Outlook Web Access.
- Non-Organisation PC or laptop using Outlook Web Access (Webmail client) through a web-browser.
- Organisation owned mobile device.
- Personal mobile devices which support appropriate security measures including non-removable 'at rest' encryption (See list in NHS Mail Guidance section for up to date information). The Organisation provides no support for personal devices connected to NHSmail.

6.2.2 Users must not leave their email account logged in an unprotected. If you are accessing the service using a non-trusted connection you will be automatically logged out of the service after **30 minutes** of inactivity.

6.2.3 If you are accessing the service using a trusted connection you will be logged out after a period of inactivity of **8 hours**.

6.3 Email Confidentiality and Security

6.3.1 Patient Confidential Data (PCD) should only be exchanged electronically when encrypted. NHSmail emails sent to secure domains is automatically encrypted and complies with the pan-government secure email standard NHSmail is accredited to the NHS secure email standard and is suitable for sharing patient identifiable and sensitive information.

When sending emails outside of NHSmail, use [secure] at the start of the email subject. [Secure] is not case sensitive. The NHSmail service will assess whether encryption is required.

- If the domain the email is being sent to is accredited, the email will be sent securely and no further encryption is required.
- If the domain the email is being sent to is not accredited, and therefore insecure, the NHSmail service will programmatically enforce the use of the encryption tool to protect the email data. The recipient will need to log into the Trend Encryption Micro portal to unencrypt the email before it can be read.
- The Cabinet Office and NHS Digital will hold a list of all the domains that are accredited which NHSmail will refresh on a daily basis to ensure that emails are encrypted as required.

Guidance is available on how to use the NHSmail encryption service.

6.3.2 Trusted and non-trusted connections

Users should generally access email from "trusted" connections, however, mobile working arrangements acknowledge that email may be accessed through non-trusted connections.

Users should be aware of, and are responsible for, applying appropriate controls to mitigate identified risks.

A trusted connection is access to NHSMail made using a computer attached to the N3 or GSi network. Access to NHSMail is automatically secured when accessing NHSMail from a workstation sited in the Vale of York offices or Vale of York issued laptop using a remote access server token and password.

GSi is the Government Secure Intranet. It is a government network that can be used for secure electronic communication between government organisations.

Secure email domains in Central Government:

- .gsi.gov.uk
- .gse.gov.uk
- .gsx.gov.uk

The Police National Network/Criminal Justice Services secure email domains:

- .pnn.police.uk
- .scn.gov.uk
- .cjsm.net

Secure email domains in Local Government/Social Services:

- .gcsx.gov.uk

Email sent to / from NHSmail addresses and email addresses ending in the above will be secure in transit. The Government is expanding GSi coverage and access to other public sector organisations and the list above may increase.

When sending outside the GSi network, personal, sensitive and confidential information must be removed from the subject line and body text of the document and sent as an encrypted attachment.

Anything other than N3 or GSi is considered to be a non-trusted connection. For example, when you log in from home or an internet cafe. eMBED Information Governance team is happy to advise on the safe transport of confidential / sensitive content to non-GSi email accounts if required

6.3.3 Statutory Disclosure of Emails

Staff should be aware that comments and information sent for personal and business purposes via the medium of NHSMail may be disclosed under subject access requests under the Data Protection Legislation and requests for information made under the Freedom of Information Act 2000 which provides a statutory right of access to all recorded information held by the CCG, subject to certain exemptions to disclosure.

6.4 Synchronisation of NHSMail with Mobile Devices

6.4.1 Users may synchronise mobile devices with their NHSMail account. Users are responsible for implementing appropriate security on the mobile devices with which NHSMail is synchronised. The CCG has standardised on the provision of Apple iPhones for key workers. Apple iPads may also be provided for some staff. Mobile devices connecting to NHSmail must adhere to the NHSmail mobile device policy which is automatically applied:

- A password must be applied to unlock the device;
- An inactivity timeout should be set that requires the input of a password to unlock the device or if the device goes into standby mode;
- If an incorrect password is entered eight times in succession, the phone is automatically wiped of ALL data and restored to its default factory settings.

6.4.2 Email messages on mobile devices are automatically restricted to a maximum message size is 500KB. Messages over this size (20MB) may be received in your NHSmail mailbox but not on a mobile phone.

- Only one month's worth of email is synchronised with devices to reduce the risk of data loss as well as improve synchronisation times / reduce cost
- The device password must be changed every 90 days
- Encryption at rest should be enabled on devices with the built-in capability to support it. (Encryption at rest on the iPhones is built-in and already enabled by default with no ability to turn it off. This means data is already encrypted on the phone and can only be read after the phone is unlocked by applying the password, preventing access should it fall into the wrong hands.)

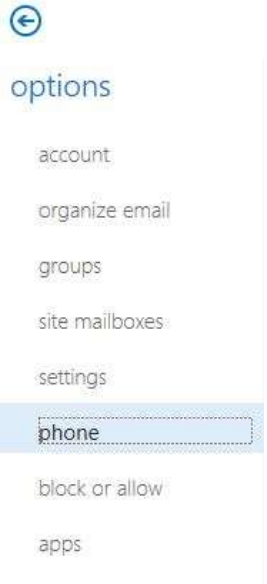
6.4.3 In the event of the device getting lost, stolen, misplaced or updated, it is the responsibility of the device holder to manage the 'remote wipe data' through NHSmail. IT support is available if needed. Remote wiping is done by following these steps :

Log in to NHSmail at www.nhs.net

Follow step 1-3:

1 Click options

2. Click Mobile Devices



3. Click Wipe All Data from Device

6.4.4 iCloud Service

Apple has provided an iCloud service. iCloud means that data on mobile devices may be stored in a cloud based storage facility and the content is synchronised to and from your device over a wireless internet connection. If your device is configured to use iCloud and access NHSmail account, the user is responsible for ensuring that email is not set up to be synchronised to the iCloud service. This is important as synchronising NHSmail to the iCloud service means that any confidential, sensitive or person identifiable data will be transmitted over a potentially unsecured wireless network and hosted in Apple servers, putting sensitive data at risk. Data stored on iCloud cannot be removed.

Many mobile brands offer similar facilities. Users of other types and makes of devices should be similarly aware of the risks of backing up mobile device data online.

6.5 Opening Email attachments

Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus software although occasionally, as with any email service, a new virus may not be immediately detected. If you are

unsure of the source of an email or attachment you should leave it unopened and inform the eMBED IT services team. Users of NHSMail are responsible for managing received mail and attachments. Staff should not introduce or forward any virus or any other computer programme that may cause damage to NHS computers or systems. Staff will be held responsible for any deliberate introduction of malware that causes any loss of service.

6.6 Management of Email

6.6.1 There is a common misconception that email messages constitute an ephemeral form of communication. This misconception about how email messages can be used could result in legal action being taken against eMBED or individuals. All email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. Staff should also be aware that email messages could be used as evidence in legal proceedings.

6.6.2 There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example holiday or sickness. Whilst users are entitled to expect a level of privacy in relation to their e-mail correspondence they must understand that this will not be an absolute right and that the needs of the organisation may override it in certain circumstances. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the Data Protection Legislation
- Freedom of Information request
- Evidence in legal proceedings
- Evidence in a criminal investigation
- Line of business enquiry
- Evidence in support of disciplinary action

Where it is not possible to ask the permission from the member of staff whose mailbox needs to be accessed, the procedure for gaining access their mailbox is:

- Gain authorisation from Head of Department.
- Submit a request to IMT Help Desk.
- Request must be authorised in IMT by senior manager.
- A record is made of the reasons for accessing the mailbox together with the names of the people who were present.
- Inform the person whose mailbox was accessed at the earliest opportunity.

It is less likely that this procedure will need to be followed if email records are managed appropriately or mailbox access has been delegated to a trusted third party.

6.7 Inappropriate use of Email

6.7.1 The use of e-mail in the following types of activities is specifically prohibited.

- Illegal, fraudulent, or malicious activities.

- Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with eMBED.
- Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.
- Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.
- Viewing, damaging, or deleting files or communications belonging to others without appropriate authorisation or permission.
- Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.

6.7.2 These, and other inappropriate activities, may result in disciplinary action being taken against the person found misusing the e-mail service for such purposes.

6.8 Records Management

6.8.1 Email messages can constitute part of the formal record of a transaction, decision or communication about an issue. All members of staff are responsible for identifying and managing emails messages that constitute a record of their work.

6.8.2 NHS guidance[1]provides the following information concerning the retention of emails, (Active Accounts)

Data	Retention Period	Additional Detail
Inbox, subfolders, calendar, contacts and tasks	Infinite	All identified material will be kept in perpetuity unless deleted by the user. NHS Mail Accounts can be removed by a local administrator through the 'leaver' process and in accordance with eMBED NHSMail management procedures. Once an account has been removed any residual content will be destroyed. Accounts that have not been accessed for over 24 months will be automatically removed from the service and any residual content will be destroyed.
Deleted mailbox data	14 days	Users may restore any email and calendar data they have deleted in the last 14 days. Synchronising a blank calendar from a mobile device over the server copy is not a delete (it is a replace) and as such there is no deleted data to restore. Please note that there is no user recovery process for email, calendar/tasks/contacts data outside the 14 day period.

[1] http://systems.hscic.gov.uk/nhsmail/policies/retention.pdf

6.8.3 When an email is sent or received a decision needs to be made about whether the email needs to be captured as a record. Once an email message has been captured as a record it should be deleted from the email client. The main points to consider when managing email records are :

- Identifying email records
- Who is responsible for capturing email records
- Email messages with attachments
- When to capture email records
- Where to capture email records
- Titling email records

6.8.4 Email messages with attachments. Where an email message has an attachment a decision needs to be made as to whether the email message, the attachment or both should be kept as a record. The decision on whether an email and/or its attachment constitute a record depends on the context within which they were received. It is likely that in most circumstances the attachment should be captured as a record with the email message as the email message will provide the context within which the attachment was used. There are instances where the email attachment might require further work, in which case it would be acceptable to capture the email message and the attachment together as a record and keep a copy of the attachment in another location to be worked on. In these circumstances the copy attachment that was used for further work will become a completely separate record.

6.8.5 When to capture. Email messages that can be considered to be records should be captured as soon as possible. Most email messages will form part of an email conversation string. Where an email string has formed as part of a discussion it is not necessary to capture each new part of the conversation, i.e. every reply, separately. There is no need to wait until the end of the conversation before capturing the email string as several subjects might have been covered. Email strings should be captured as records at significant points during the conversation, rather than waiting to the end of the conversation because it might not be apparent when the conversation has finished.

6.8.6 Where to capture. Email messages that constitute records should be saved on shared drives. Email messages captured as records should be located with other records relating to the same business activity. Personal mailboxes should not be used for long-term storage of email messages. Personal mailboxes should be used for personal information or short-term reference purposes, when these emails are no longer required they should be deleted.

6.8.7 Storage. Once captured and stored the e-mail becomes subject to the same standard for records retention as any other record.

6.9 Good Practice and Effective use of Email

6.9.1 The following guidelines have been included into this Standard document to provide assistance to users in the effective use of Email services.

6.9.2 Subject Line

- Ensure the subject line gives a clear indication of the content of the message
- Indicate if the subject matter is sensitive
- Use flags to indicate whether the message is of high or low importance and the speed with which an action is required
- Indicate whether an action is required or whether the email is for information only

6.9.3 Subject and Tone

- Greet people by name at the beginning of an email message
- Identify yourself at the beginning of the message when contacting someone for the first time
- Ensure that the purpose and content of the email message is clearly explained
- Include a signature with your own contact details
- Ensure that the email is polite and courteous
- Tone of an email message should match the intended outcome
- Make a clear distinction between fact and opinion
- Proof read messages before they are sent to check for errors
- Try to limit email messages to one subject per message
- Include the original email message when sending a reply to provide a context
- Where the subject of a string of email messages has significantly changed start new email message, copying relevant sections from the previous string of email messages
- Ensure email messages are not unnecessarily long
- Ensure that attachments are not longer versions of emails
- Summarise the content of attachments in the main body of the email message

6.9.4 Structure and Grammar

- Try to use plain English
- Check the spelling within the email message before sending
- Use paragraphs to structure information
- Put important information at the beginning of the email message
- Take care when using abbreviations
- Avoid using CAPITALS
- Try not to over-use bold and coloured text

6.9.5 Addressing

- Distribute email message only to the people who need to know the information.
- Using 'reply all' will send the reply to everyone included in the original email. Think carefully before using 'reply all' as it is unlikely that everyone included will need to know your reply.
- Use the 'To' field for people who are required to take further action and the 'cc' field for people who are included for information only.
- Think carefully about who should be included in the 'cc' field.
- Ensure the email message is correctly addressed.

6.9.6 General

- Be aware that different computer systems will affect the layout of an email message.
- Avoid sending email messages in HTML format.
- Be aware that some computer systems might have difficulties with attachments.
- Internal emails should use pointers to attachments and information held on shared drives or the Intranet.

6.10 User Responsibilities

6.10.1 General Responsibilities

- It is your personal responsibility to check that you are sending email to the right recipient, as NHSmail is a national system where there may be more than one person with the same name. Always check that you have the correct email address for the person you wish to send to.
- You must ensure that it is appropriate for all recipients to access the content of any email you send. Use 'reply to all' with caution.
- Emails should be treated like any other clinical / business communication and care should be taken to ensure that content is accurate and the tone is appropriate in accordance with the Organisation Values.
- You must not send any material by email that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic.
- If you need to transmit sexually explicit material for a valid clinical reason then you must obtain permission from the Information Governance Team. Where this is the case you must keep adequate records.
- Do not send email messages using another person's email account
- Your use of the NHS Mail system must be in accordance with the organisations Acceptable Computer Use Standard.

6.10.2 User Legal Responsibilities

- You must not use the CCG's email service to violate any laws or regulations of the United Kingdom or other countries.

- Use of the service for illegal activity is usually grounds for immediate dismissal and any illegal activity will be reported to the police.
- Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking, sexual harassment or treason.
- You must not attempt to interfere with the technical components, both hardware and software, of the Organisation email service in any way.
- You must not use the Organisation email service for harassment by sending persistent emails to individuals or distribution lists.
- Do not breach copyright or licensing laws when composing or forwarding emails and email attachments.
- Email is admissible as evidence in a court of law and messages are classified as legal documents. Internal emails may also need to be disclosed under the Data Protection Legislation , Freedom of Information Act (2000) and other legislation.

6.10.3 Home / Remote User Responsibilities

NHSmail may be used outside the NHS network on any computer with an internet connection. However the user is personally responsible for the information security and confidentiality of e-mail in their 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.
- Do not save confidential information on 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 other third parties.
- Passwords must be memorised, not written down.
- Log out of the NHSmail application when not in use.
- Do not leave the NHSmail application logged in when unattended.
- Maintain an awareness of relevant Organisation policies and procedures and observe these at all times.
- Never select an option that allows you to save your password for later use. Always type your password, even if you plan to use the same computer for several days.
- Only ever provide your username and password to the NHSmail website.
- If you are accessing the service using a non-trusted connection you will be automatically logged out of the service after 30 minutes of inactivity.
- If you are using a public computer, click the “Open as Web Page” link next to the attachment name. This protects you from potential virus attacks and prevents a copy of the attachment from being created and stored in the temporary files on the computer.

6.10.4 Passwords

Password security is a key component in the security of the NHSmail service. Users are responsible for ensuring that their password is kept confidential and secure at all times. Users should notify IMT Services if they become aware of any unauthorised access to their email account or if they believe that their password may have been revealed.

Passwords must be changed every 90 days, however if at any time the user has reason to suspect that password security has been breached the password should be changed immediately.

You may reset a forgotten password as long as you are using a trusted connection. If you are using a non-trusted connection you will need to contact your LOA, who can reset the password for you. An LOA cannot view your password, and you will never need to give your password to an LOA or anyone else.

If you are required to change your password on login over a trusted connection, you will be presented with a page requesting you to provide a new password. You will not be able to continue using the service until you have provided a valid new password.

An example of a trusted connection is N3, the national network for the NHS.

If you use a mobile device to access NHSmail, please ensure you change the saved NHSmail password configured on your mobile device.

I received an email from my bank/NHSmail/other web site saying I must send them my password or my account will be disabled– should I send my password, should I report it, should I log a helpdesk call?

This kind of email is known as a 'Phishing email' and is a criminal or fraudulent attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. You should not in any circumstances respond to these emails.

6.10.5 Generic / Departmental Email Address

Generic mailboxes should be used where there are a group of people responsible for the same area of work to ensure that queries are answered quickly when members of the team are away from the office. Requests for the setting up of generic mailboxes must come to the Business Support Manager following on from the approval for the relevant head of department. It will then be forwarded to the IMT Service Desk for creation. Access to the generic mailbox will be setup for the designated owner and it is this person's responsibility to manage and delegate access for other staff members.

6.10.6 Email Forwarding

Email communication sent from the CCG email service to any non-NHS Mail or non GSi email account is insecure. Unencrypted person-identifiable and / or sensitive information must never be sent outside the NHS N3 or .GSi public sector network,

either automatically or as a result of re-direction or directly. To do so is in direct contravention of NHS and Government data security requirements, and has been a prohibited practice since February 2008.

Email auto-forwarding to non-NHSMail addresses is prohibited by Information Governance rules. The Information Governance team are happy to advise on the safe transport of confidential / sensitive content to non-Organisation email accounts if required.

6.10.7 Email Delegation

Passwords to NHSmail must not be shared (other than where specific authorisation has been given for technical reasons). The Organisation email service allows users to delegate permissions to their own email account and calendar.

6.10.8 Personal Use

Organisation email services are established to help with the provision of health and social care and this should be the main use of the service. The Organisation allows the reasonable use of email for personal use if certain guidelines are adhered to:-

- Personal use of email must not interfere with work.
- Personal emails must also adhere to the guidelines in this Standard.
- Personal emails are kept in a separate folder, named 'Private'. The emails in this folder must be managed.

6.10.9 Private Business Use

The use of NHSmail and other resources for non-healthcare business is not permitted.

6.10.10 System Monitoring

All emails are monitored for viruses.

All email traffic (incoming and outgoing) is logged automatically. These logs are audited periodically. The content of emails are not routinely monitored. However, the Organisation reserves the right to retain and review message content as required to meet organisational, legal and statutory obligations. Breach of this Standard may have contractual consequences for members of staff and could lead to legal action being taken against individuals and / or the Organisation.

6.10.11 Organisation wide Emails

Users are limited to sending out emails to a maximum of 200 users. Access to distribution lists such as "all staff" is restricted to Directors, their PA's and certain specific post holders. This facility must be used with due care and consideration.

6.10.12 Standard Adherence

The Organisation does not require a signed document from email users. All email users are responsible for ensuring that they understand and comply with the

contents of this Standard. Individual's use of organisation computing equipment demonstrates their consent to the terms of this Standard.

6.11 Internet / Intranet Access

6.11.1 Access is provided to the internet through a secure gateway operated by IMT. eMBED operates a secure firewall and a range of technical systems to attempt to reduce the risk posed by hackers, criminals and fraudsters who may attempt to attack our systems.

Internet connectivity is provided to facilitate a person's work at the CCG. Access is also encouraged to facilitate and improve health service management activities. Commercial work is unacceptable.

6.11.2 As a secondary use users are permitted to utilise the system for their own personal use subject to compliance with the policy. Users are advised that this personal use is classed as a privilege which can be removed and is also subject to monitoring.

6.11.3 Monitoring. Users are advised that all computer use, including e-mail and internet access is monitored and that staff are advised that in accordance with the Employment Practices Data Protection Code monitoring of Internet use will take place subject to the following guidance :

- Monitoring and IT Security Audit will be carried out by the Information Governance Team.
- All audits carried out will be documented.
- Monitoring is required to ensure that employees do not breach any regulations (such as those on harassment) which could have a legal impact on eMBED.
- Spot checks will be done as opposed to continuous monitoring.
- Traffic will be monitored as opposed to content unless there are reasons for doing otherwise.
- The History folder on a local computer is to be set to retain information for 20 days (this is the default setting). Users are not to clear, delete or otherwise change the settings on the History Folder on their PC. Such action may lead to further detailed examination of the system being necessary.
- Inappropriate use of the Internet services may result in either facility being withdrawn and may constitute an offence under the NHS disciplinary code.

6.11.4 Software must not be downloaded from the Internet without authorisation from the IT Services Department. This excludes information files from NHS related sites.

6.11.5 Making material available via the Internet, which may be offensive, obscene or abusive i.e. adult, pornographic material, is not acceptable, and may render the perpetrator liable to prosecution under UK law.

6.11.6 Suspicion that a staff member has either attempted to, or indeed has successfully accessed Pornographic, Adult and other "unsuitable" sites will lead to the withdrawal of service for the individual concerned, and possible disciplinary action being taken, in accordance with the CCG Disciplinary Policy.

6.12 Social Media

6.12.1 Social media means web-based tools which allow users to communicate with each other across the worldwide web. This includes :

- Microblogging – for example, Twitter.
- Blogging – for example, WordPress and Tumblr.
- Video sharing – for example, Flickr and Instagram.
- Social Bookmarking – for example, Pinterest, Reddit and StumbleUpon.
- Social sharing – for example, Facebook, Snapchat.
- Professional sharing – for example, Linkedin.

Social media is a 'real time' communications channel that communicates in "real time" which brings opportunities and threats. The CCG has adopted a "common-sense" approach to managing potential risks while developing our involvement.

6.12.2 CCG Statement

The CCG will use social media to help achieve the criteria set out in our vision. We will use this channel to receive feedback from people within our commissioning area, and from our colleagues in the NHS.

6.12.3 Staff Responsibilities

All messages or videos that are to be published on social media websites, should be checked by the CCG Communications Team. The CCG Communications Team manages the organisation's social media presence and output.

6.12.4 Employees using social media *on behalf of the CCG* should:

- 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 they are an ambassador for the CCG;
- be responsible and be honest at all times;
- share insight or information gained 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 your communications advisor if in doubt; and
- stay within the law and be aware that libel, defamation, copyright and data protection laws apply.

6.12.5 Individuals using social media ***privately*** should be careful not to make comments or post material which bring themselves, the CCG or individuals working for the CCG into disrepute. 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.

6.12.6 Guidelines for Using Social Media

When using social media staff are responsible for their online image and how this portrays the Vale of York Clinical Commissioning Group. Staff must take the following into consideration:

- Know and adhere to Vale of York CCG policy and procedures;
- Understand personal responsibilities to stay within the law and not bring the Vale of York Clinical Commissioning Group or the wider NHS into disrepute.
- Respect copyright, 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 the CCG.
- Don't cite or reference colleagues, services or organisations without their approval. When you do make a reference, where possible link back to the source.
- 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.

Although it is acceptable for staff to say they work for the NHS or CCG in posts and during online conversations; they should ensure their personal online profile carries the following disclaimer: "The postings on this site are my own opinion and don't necessarily represent NHS or CCG policy or opinion".

Incidents of discrimination, bullying or harassment which take place via social media will be managed in line with CCG Disciplinary Policy.

6.12 Introduction and Applicability

6.13.1 Acceptable Use statements apply to anyone using CCG IT systems, computer equipment and network services. This includes employed staff, temporary staff and contractors granted access, including access to the guest wireless. eMBED manages an IT network infrastructure which covers a number of NHS organisations, including Vale of York Clinical Commissioning Group and has set standards which protects employees, customers and other partners from harm caused by the misuse of IT systems and loss/misuse of data. Misuse includes both deliberate and inadvertent actions.

6.13.2 The repercussions of misuse of IT systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime. Everyone who works at the CCG is responsible for the security of the IT network infrastructure and systems and the data on them. As such, all employees must ensure they adhere to these guidelines at all times. Should any employee be unclear how this impacts their role they should speak to their manager or the eMBED Information Governance Team.

6.13.3 Systems" means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked

devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

6.13.4 Virus Protection. eMBED IMT Services will ensure that the appropriate technical steps are taken to reduce the vulnerability of the system to attack from computer viruses. Users are expected to play their part by being aware of the problem of viruses and reporting anything they deem to be suspicious to the IT Helpdesk.

6.13.5 Passwords. Users must follow the required standard for passwords:

- Change your password every three months.
- Never share your password
- Never reveal your password to anyone
- Don't write your password down
- If you suspect that your password has been compromised, report the matter to the Service Desk immediately

6.14 Inappropriate Use of Computer / IT Services

The use of computers and internet services in the following types of activities is specifically prohibited :

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with the CCG.
- Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.
- Viewing, damaging, or deleting files belonging to others without appropriate authorisation or permission.
- Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.
- Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.
- Plugging in personal equipment into a work device
- Accessing Non-work related third party applications from work devices
- Accessing personal email systems or personal social media accounts from work devices

7 POLICY IMPLEMENTATION

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

8 TRAINING AND AWARENESS

8.1 This policy will be published on the CCG's website and will also be available to staff on the organisation's intranet.

The policy will be brought to the attention of all new employees as part of the induction process. Further advice and guidance is available from the Business Support Manager.

9 MONITORING AND AUDIT

9.1 Users are advised that all computer use, including e-mail and internet access is monitored and that staff are advised that in accordance with the Employment Practices Data Protection Code monitoring of Internet use will take place subject to the following guidance :

- Monitoring and IT Security Audit will be carried out by the Information Governance Team.
- All audits carried out will be documented. Monitoring is required to ensure that employees do not breach any regulations (such as those on harassment) which could have a legal impact on the CCG.
- Traffic will be monitored as opposed to content unless there are reasons for doing otherwise.
- Inappropriate use of the Internet services may result in either facility being withdrawn and may constitute an offence under the CCG disciplinary Policy .
- Spot checks will be done as opposed to continuous monitoring.

10 POLICY REVIEW

10.1 This policy will be reviewed in two years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation / guidance.

11 REFERENCES

- Data Protection Act 2018
- General Data Protection Regulation
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Caldicott Principles

- NHS Code of Practice: Information Security Management
  http://systems.hscic.gov.uk/nhsmail/policies/retention.pdf

12 ASSOCIATED POLICIES

- IG02 Data Protection and Confidentiality Policy
- IG04 Freedom of Information Policy
- IG05 Information Security Policy
- IG06 Information Risk Policy
- IG07 Corporate Records Management Standards and Procedures
- IG08 Mobile Working Policy
- IG09 Subject Access Request Policy
- IG10 Safe Haven Policy
- IG11 Information Governance Strategy

13 CONTACT DETAILS

The Governance Team
VOYCCG.Governance@nhs.net
NHS Vale of York Clinical Commissioning Group
West Offices
Station Rise
York, YO1 6GA

NHS
Vale of York
Clinical Commissioning Group

14 APPENDIX 1 : EQUALITY IMPACT ANALYSIS FORM

1.	**Title of policy/ programme/ service being analysed**
	Email, Internet and Acceptable Use Policy
2.	**Please state the aims and objectives of this work.**
	This policy provides guidance on the CCG's expectations for the use of the internet and email.
3.	**Who is likely to be affected? (e.g. staff, patients, service users)**
	Staff need to comply with the principles and practices outlined in this policy.
4.	**What sources of equality information have you used to inform your piece of work?**
	NHS England guidance
5.	**What steps have been taken ensure that the organisation has paid due regard to the need to eliminate discrimination, advance equal opportunities and foster good relations between people with protected characteristics**
	The analysis of equalities is embedded within the terms of reference of the CCG's committees and project management framework.
6.	**Who have you involved in the development of this piece of work?**
	Internal involvement : Senior Management Team **Stakeholder involvement** : Consultation with Senior Managers **Patient / carer / public involvement** : This is an Internal policy aimed at staff employed by the CCG and contractors working for the CCG. The focus is on compliance with statutory duties and NHS mandated principles and practice. There are no particular equality implications.
7.	**What evidence do you have of any potential adverse or positive impact on groups with protected characteristics?** **Do you have any gaps in information?** **Include any supporting evidence e.g. research, data or feedback from engagement activities**

Disability People who are learning disabled, physically disabled, people with mental illness, sensory loss and long term chronic conditions such as diabetes, HIV)	Consider building access, communication requirements, making reasonable adjustments for individuals etc.
N/A	
Sex Men and Women	Consider gender preference in key worker, single sex accommodation etc.
N/A	
Race or nationality People of different ethnic backgrounds, including Roma Gypsies and Travellers	Consider cultural traditions, food requirements, communication styles, language needs etc.
N/A	
Age This applies to all age groups. This can include safeguarding, consent and child welfare	Consider access to services or employment based on need/merit not age, effective communication strategies etc.
N/A	
Trans People who have undergone gender reassignment (sex change) and those who identify as trans	Consider privacy of data, harassment, access to unisex toilets & bathing areas etc.
N/A	
Sexual orientation This will include lesbian, gay and bi-sexual people as well as heterosexual people.	Consider whether the service acknowledges same sex partners as next of kin, harassment, inclusive language etc.
N/A	
Religion or belief Includes religions, beliefs or no religion or belief	Consider holiday scheduling, appointment timing, dietary considerations, prayer space etc.
N/A	

Marriage and Civil Partnership Refers to legally recognised partnerships (employment policies only)	Consider whether civil partners are included in benefit and leave policies etc.
N/A	
Pregnancy and maternity Refers to the pregnancy period and the first year after birth	Consider impact on working arrangements, part-time working, infant caring responsibilities etc.
N/A	
Carers This relates to general caring responsibilities for someone of any age.	Consider impact on part-time working, shift-patterns, options for flexi working etc.
N/A	
Other disadvantaged groups This relates to groups experiencing health inequalities such as people living in deprived areas, new migrants, people who are homeless, ex-offenders, people with HIV.	Consider ease of access, location of service, historic take-up of service etc.
N/A	

8.	**Action planning for improvement** Please outline what mitigating actions have been considered to eliminate any adverse impact? No adverse equality impact has been identified. Please state if there are any opportunities to advance equality of opportunity and/ foster good relationships between different groups of people? An Equality Action Plan template is appended to assist in meeting the requirements of the general duty

Sign off
Name and signature of person / team who carried out this analysis Business Support Manager
Date analysis completed 13 September 2017
Name and signature of responsible Director
Date analysis was approved by responsible Director

15 APPENDIX 2 : SUSTAINABILITY IMPACT ASSESSMENT

Staff preparing a policy, Governing Body (or Sub-Committee) report, service development plan or project are required to complete a Sustainability Impact Assessment (SIA). The purpose of this SIA is to record any positive or negative impacts that this is likely to have on sustainability.

Title of the document	Email, Internet and Acceptable Use Policy
What is the main purpose of the document	This policy provides guidance on the CCG's expectations for the use of the internet and email.
Date completed	13 September 2017
Completed by	Business Support Manager

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced ?
Travel	Will it provide / improve / promote alternatives to car based transport?	0		
	Will it support more efficient use of cars (car sharing, low emission vehicles, environmentally friendly fuels and technologies)?	0		
	Will it reduce 'care miles' (telecare, care closer) to home?	0		
	Will it promote active travel (cycling, walking)?	0		
	Will it improve access to opportunities and facilities for all groups?	0		
	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced ?
Procurement	Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives?	0		
	Will it promote ethical purchasing of goods or services?	0		
Procurement	Will it promote greater efficiency of resource use?	0		
	Will it obtain maximum value from pharmaceuticals and technologies (medicines management, prescribing, and supply chain)?	0		
	Will it support local or regional supply chains?	0		
	Will it promote access to local services (care closer to home)?	0		
	Will it make current activities more efficient or alter service delivery models	0		
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled? Will it reduce water consumption?	0		
Workforce	Will it provide employment opportunities for local people?	0		
	Will it promote or support equal employment opportunities?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced ?
	Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies)?	0		
	Will it offer employment opportunities to disadvantaged groups?	0		
Community Engagement	Will it promote health and sustainable development?	0		
	Have you sought the views of our communities in relation to the impact on sustainable development for this activity?	N/A		
Buildings	Will it improve the resource efficiency of new or refurbished buildings (water, energy, density, use of existing buildings, designing for a longer lifespan)?	0		
	Will it increase safety and security in new buildings and developments?	0		
	Will it reduce greenhouse gas emissions from transport (choice of mode of transport, reducing need to travel)?	0		
	Will it provide sympathetic and appropriate landscaping around new development?	0		
	Will it improve access to the built environment?	0		

Domain	Objectives	Impact of activity Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = N/A	Brief description of impact	If negative, how can it be mitigated? If positive, how can it be enhanced ?
Adaptation to Climate Change	Will it support the plan for the likely effects of climate change (e.g. identifying vulnerable groups; contingency planning for flood, heat wave and other weather extremes)?	0		
Models of Care	Will it minimise 'care miles' making better use of new technologies such as telecare and telehealth, delivering care in settings closer to people's homes?	0		
	Will it promote prevention and self-management?	0		
	Will it provide evidence-based, personalised care that achieves the best possible outcomes with the resources available?	0		
	Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways?	0		

16. APPENDIX 3 : THE CCG'S SOCIAL MEDIA ACCOUNTS

The CCG uses the following social media accounts, which are run by the communications and media relations team.

- **Twitter** @ValeofYorkCCG https://twitter.com/ValeofYorkCCG
- Instagram valeofyorkccg https://www.instagram.com/valeofyorkccg/
- YouTube NHS Vale of York Clinical Commissioning Group https://www.youtube.com/channel/UC69gBhmiPRD80NoIH7XzOeg

Please note that any other social media account with ValeofYorkCCG or VoYCCG in its name are in no way officially affiliated with the CCG or endorsed by the CCG.

Social media house rules

We want everyone to feel as confident and comfortable as possible when interacting with our social media pages, and these guidelines have been produced accordingly.

We reserve the right to change these house rules at any point, and without notice. If they are important to you, please check back regularly.

Responding to messages

The CCG's social media accounts are monitored between 9am and 5pm Monday to Friday, although posts are also scheduled to appear on our channels at times outside of these hours.

We read all mentions, replies, posts and direct messages sent to us and assess whether to respond or not on social media. We welcome feedback and ideas from all our followers, but we may not be able to reply individually to ever message we receive on our various social media channels.

We may ask you to provide an email address in order to give you a full response, outside of the character limits imposed by the social media platforms we use.

We don't answer clinical or medical questions, but will signpost where to get information, advice or support as appropriate; nor do we discuss any individual's care through social media.

Anyone wishing to discuss their care should contact our Patient Relations team by email VOYCCG.PatientRelations@nhs.net or by phone 01904 555999.

Following and liking

The CCG follows accounts that are relevant to, or interested in, the services we commission.

We will share content which we believe is of interest to our followers, including from the accounts of individuals, companies, health organisations, other commercial enterprises and the media (and/or their employees) who have an interest in NHS Vale of York CCG and our work.

By sharing other social media users' content, our organisation does not endorse the information or others' views of that organisation or individual.

Moderating
While it's likely that the CCG will face scrutiny and criticism on social media and may even be the target of messages about wider NHS or health issues, we believe that people are entitled to air their views on social media and we wouldn't remove a post simply because it was negative.

We will, however, consider removing and/or reporting posts which :

- Contain hateful or discriminatory comments regarding race, ethnicity, religion, gender, disability, sexual orientation or political beliefs
- Contain swearing or other profane, defamatory, offensive or violent language
- Directly troll a member of staff
- Any posts that name CCG members of staff, without their permission
- Any content that is primarily aimed to discredit the CCG, or its staff, without justification
- We believe are trolling or are deliberately disruptive statements meant to hijack comment threads or throw discussions off-track
- Are attacks on specific groups
- We believe are comments meant to harass, threaten or abuse an individual
- Imply intent to stalk an individual or collect private information without disclosure
- Contains links or comments containing sexually explicit content material
- Is spam, including any comment of a promotional or commercial nature. Including profile pictures and user IDs
- Contains any personal details e.g. phone numbers, addresses etc.
- Contains downloadable files, including links to them
- Discusses illegal activity
- Relates to confidential or personal information
- Is personal promotion

If you do not want to comply with these house rules then you must not post or comment on our social media channels.

By using these sites you accept, and agree to abide by, both our rules and the terms and policies of the specific social media channel.

Email voyccg.communications@nhs.net in the event that you have seen content or comments posted on our social media channels that you believe is not in accordance with either this guidance or the terms and policies of the social media channel concerned.

Posts from CCG staff on personal accounts

Some NHS Vale of York CCG staff tweet/post from their own accounts. Their tweets / posts do not represent the official position of the CCG, and should only be considered the views and opinions of each individual.

- Individuals have right to protection of personal data which is why the CCG is required to gain written consent to take and use photographs of people in all of its publications.
- This also goes beyond the CCG as an organisation. Anyone identifying themselves on social media as being an employee of the CCG needs to be very careful to avoid any personal data breaches.
- It is very important to remember that any tweet, posting or sharing which may contain personal information (pictures or otherwise) requires consent from the individual involved first.
- If tweets, posts or shares do not contain personal information, then consent is not required.

Twitter and CCG employees

- If an employee identifies themselves as an employee of the CCG on Twitter then the duty of the CCG is extended to the individual's twitter account.
- The CCG has a duty to report certain types of personal data breaches to the relevant authorities (Information Commissioners Office etc.).

Using photographs on social media

- Photographs constitute personal data if the person/s are identifiable in the photograph. This could be used to identify the individual or something contextual e.g. working in the CCG. It could also be personal data if an individual is the focus of the image i.e. not inadvertently in the background or a photo of a crowd.
- A person can give consent for their picture to be used in CCG publications but this does not mean that they give their consent for it to be used in social media and without this consent there could be a potential breach of personal information.
- In all, there must be a legal basis for publication or social media, which is a written consent.

Retweeting / sharing photographs

- Retweeting or sharing a photograph is republication and consent from the person / persons in the photograph must be sought.
- You must have consent for processing of personal data (photograph).
- Without this there could be a breach of personal data.