NHS
Herefordshire and Worcestershire
Clinical Commissioning Group

Personal Information Security Responsibilities

Information Security Policy

Document Reference Information

Version:	1.0
Status:	Ratified
Author:	Alicia Dunsby
Directorate responsible:	Digital
Directorate lead:	Director of Digital Strategy and Infrastructure
Ratified by:	Clinical Executive Commissioning Commitee
Date ratified:	1st July 2020
Date effective:	1st July 2020
Date of next formal review:	3 years from effective date
Target audience:	All permanent and temporary employees of the CCG, Governing Body members, contractors, agency staff.

Version Control Record

Version	Description of change(s)	Reason for change	Author	Date
0.1	First draft	First draft	Alicia Dunsby	01/02/2020
1.0	Final for sign off	Reviews by Alicia Dunsby, Lolu Adjenii and Tony Cirello, including alignment with Home Working Policy	Alicia Dunsby	24/06/2020

Contents

1. Purpose

The purpose of this document and its associated policy "Herefordshire & Worcestershire CCG Corporate Information Security Policy" are to inform those personnel in scope of their responsibilities for contributing to the security of the information we work with and the standards of acceptable use for computing and the use of communications devices or systems.

2. Scope

This document applies to all employees of Herefordshire & Worcestershire CCG and also applies to secondees, workers and contractors engaged to provide a service to the organisation, either contracted directly to Herefordshire & Worcestershire CCG, contracted via agencies or contracted via a third party.

3. Definition

Herefordshire & Worcestershire CCG Corporate Information Security Policy, together with this standard is the minimum standard for acceptable use which should be applied whenever those individuals in scope access Herefordshire & Worcestershire CCG's or its partners' information, facilities and equipment.

In addition, local procedures, standards and work instructions may be defined to allow flexibility of organisational practices. This policy provides a minimum requirement to be met under nationally recognised standards.

4. Terms

- **Information Security** is about avoiding harm to people, customers or our business by protecting the information we use. This is achieved by considering:
  - ✓ **Confidentiality** - Information held by Herefordshire & Worcestershire CCG must only be seen by those who are authorised.
  - ✓ **Integrity** - Information used and provided by Herefordshire & Worcestershire CCG can only be modified by those authorised to do so and it is accurate, up-to-date and relevant.
  - ✓ **Availability –** Information required is accessible when needed.

- **Computing and communications devices or systems** for the purposes of this standard encompasses all those devices and applications normally used to access, store, create or transmit information. Examples are: desktop computer, laptop, tablet, mobile phone, smartphone, telephone, digital camera, digital video recorder, internet access, e-mail, social networking sites, applications, mobile apps and removable storage and network storage.

- **The EU General Data Protection Regulation (GDPR**) requires any organisation that processes data on identifiable living people to comply and be able to

demonstrate compliance with the six enforceable principles. GDPR gives control to citizens and residents over their personal data and simplifies the regulatory environment for international business by unifying the regulation within the EU. It is important to protect physical and electronic records which either contain Personally Identifiable Information (PII) or information which can likely lead to the identification of an individual. GDPR covers a number of areas such as citizen records, websites, internet activity, recruitment and selection of staff, employment records, information about employees' health and CCTV systems or information which together with other information in the possession of the received of that information could lead to the identification of an individual.

- The **Data Controller** (also known as **Information Asset Owner** or **Owner)** is a DPA term and is the role or group accountable for the management of the information. This is not to be confused with the **Subject** which is the person or object being described by the information.
- **Information Classification** is the act of deciding the sensitivity of the information asset. This is usually done by the information owner considering the harm/consequence if the information asset were lost, stolen or disclosed without authorisation.
- Appropriate **Information Handling** is the set of actions which are associated with a classification.

5. Responsibilities and Acceptable Use

5.1 General Principles

The following standard sets out arrangements with regard to Herefordshire & Worcestershire CCG's expectation concerning the security of the information we use, the environment in which we work and the use of computing and communications devices or systems. You must treat paper-based and electronic information with equal care.

Herefordshire & Worcestershire CCG maintains a set of information security policies on our Intranet.

The key documents are:

- **Herefordshire & Worcestershire CCG Corporate Information Security Policy** which describes our commitment to protecting the information in our care.
- **Herefordshire & Worcestershire CCG Personal Information Security Responsibilities** (this document) which describes the acceptable use of systems and how all contribute to information security.
- **Herefordshire & Worcestershire CCG Information Governance, Data Security and Protection Policies and Information Governance Handbook**

This is not a definitive list of the policies and procedures to which you should adhere.

Herefordshire & Worcestershire CCG policies are published on our website and intranet and you should speak to your manager for further advice.

5.2 Office Security

5.2.1 IDs and Door Access

Everyone requiring regular access to Herefordshire & Worcestershire CCG offices and on terms longer than two weeks should be issued with a Herefordshire & Worcestershire CCG ID badge for identification and access via doors protected with electronic locks.

Whilst on work premises or representing Herefordshire & Worcestershire CCG at customer sites you must be in possession of and display a valid Herefordshire & Worcestershire CCG ID badge. You must not loan your ID badge to others.

If an ID badge is lost or stolen it must be reported to the Business Support team as soon as possible. They will disable the door access associated with your current card and a replacement will be issued.

If you have lost or forgotten your ID badge you must obtain a temporary door pass for that day. Temporary door passes are available from the Business Support teams at Herefordshire & Worcestershire CCG premises. These must be signed for, should be returned at the end of each day and must not be used as a long-term alternative to an ID badge.

At the end of your employment contract your Herefordshire & Worcestershire CCG ID credentials must be returned to your manager or their representative.

Redundant ID badges which have either been replaced in the event of a loss or returned at the end of employment must be returned to Business Support teams at Herefordshire & Worcestershire CCG premises for destruction.

Be aware of who is entering a security door behind you when you enter/leave the office. If they are unaccompanied by an employee and you do not recognise them please politely ask who they are here to see and follow the visitors procedure detailed below.

People wanting to gain unauthorised access to our offices could wait for an authorised person or group of employees and try to follow them through secure doors (tailgating), or look for opportunities where the door does not close promptly. Be aware that these represent a risk to the security of our offices and report suspicious behaviour.

Do not prop open doors to secure areas and leave them unattended.

Do report any broken door or window locks to the person responsible for maintenance immediately.

If you open a window remember to close it at the end of each day. If you are the last one in your area of the office or a meeting room, check and close all windows and any exterior doors before you leave.

Key Holders are not permitted to give or loan their key to any unauthorised person without written agreement from a senior manager. Apart from the obvious security risks, any person who loses a key for the premises must report the loss to the senior manager of the relevant business area as soon as they become aware that they are missing.

5.2.2 Visitors/Sign in Procedure

The visitors procedure is in place to ensure the safety and security of all those who work for Herefordshire & Worcestershire CCG as well as ensuring we present a professional image to any visitors coming to the office.

When a visitor arrives at our offices the host should be informed of their arrival and be asked to collect them from reception ensuring that their visitor has signed in and been given a visitor's ID badge or label, if required a visitor door pass can also be issued.

If you are receiving visitors you are responsible for hosting them whilst they are in our offices. In general visitors should not be left to wander or "find their way" around our offices. You will consider the work of colleagues, the context of the visit and security of our information before deciding on the level of supervision needed and who should be made aware of their presence.

It is also your responsibility to ensure that visitors on leaving our offices have signed out and returned their visitor's ID or label and door pass and are not left to find their own way out.

Should you notice a visitor in the office without an ID or label, politely ask who they are here to see, request that they sign into the visitor's book, display their badge at all times, and guide them immediately to the appropriate person.

5.2.3 Clear Desk Policy & Printing

When deciding whether something is confidential or sensitive, consider the impact of the item(s) received by someone unauthorised to handle such information. Choose caution over convenience.

To help maintain confidentiality Herefordshire & Worcestershire CCG enforces a "Clear Desk Policy". This means that you are to tidy your desk at the end of each working day ensuring that:

- All protectively marked items (documents, CDs, DVDs, storage devices such as USB drives) owned by Herefordshire & Worcestershire CCG or any NHS providers containing sensitive personally identifiable information will be stored out of sight when the area is unattended, ideally locked in a secure environment.

- No protectively marked Herefordshire & Worcestershire CCG or provider information or sensitive personally identifiable information should be available for casual viewing or inspection by those unauthorised to see the information, such as customers, suppliers, visitors or cleaners.
- All protectively marked Herefordshire & Worcestershire CCG and provider documents or documents with sensitive personally identifiable information must be placed in secure waste bins when no longer required.

Secure print is the facility whereby to retrieve your document from the printer a PIN or ID must be used. This facility is currently available throughout Herefordshire & Worcestershire CCG offices and should be used exclusively where available.

- If using a shared printer without secure print, documents must be collected immediately to prevent theft or unauthorised viewing.
- If printing a sensitive document to a shared printer or a printer in a common area (i.e. not used exclusively by people who would normally have access to that information) wait for the print to finish, do not leave it unattended.
- When collecting prints, especially when sending to customers or a third party always check the information is complete, relevant to the recipient and does not inadvertently include information intended for someone else.
- Printing defaults should be black and white and duplex.
- Printing your personal documents using Herefordshire & Worcestershire CCG equipment in general is not permitted. If required authorisation must be obtained from your line manager.

5.3 Computer Use

No exhaustive list can be prepared defining all possible forms of misuse of computing and communications devices or systems. The individual circumstances of each case will need to be taken into account. However, some examples are outlined below:

- Use of computing resources for improper, immoral, fraudulent or unlawful purposes or to access, store, create or transmit any material which is offensive, abusive, indecent, defamatory, obscene, or menacing. For example sexually explicit material or offensive statements based upon race, sex, sexuality, disability, age or religion.
- Storing/loading/executing of software for a purpose which is not work related.
- Storing/loading/executing of software:
  - ✓ which has not been acquired through approved Herefordshire & Worcestershire CCG procurement procedures, or
  - ✓ for which Herefordshire & Worcestershire CCG does not hold a valid program licence, or
  - ✓ which has not been the subject of formal virus checking procedures
- Storing/processing/printing of information for a purpose which is not work related.

5.3.1 Obtaining Computer Equipment and Software

Herefordshire & Worcestershire CCG will provide you with the equipment and software needed to do your job.

The configuration and delivery of all Herefordshire & Worcestershire CCG IT equipment and software is conducted by the organisation's IT Service provider.

The purchase of all Herefordshire & Worcestershire CCG IT equipment and software is processed through the organisation's IT Service provider procurement. Any physical hardware will be labelled with the organisation's asset tag for identification.

Queries on IT procurement should be sent to Alicia.dunsby@nhs.net

Asset Stickers must not be removed from our equipment. If damaged or unreadable contact your local IT Service Desk.

Loss of equipment or faults with any supplied hardware or software must be raised with your local IT Service Desk as soon as possible.

5.3.2 Credentials and Systems Access

It is a criminal offence under the Computer Misuse Act, 1990 to deliberately attempt to access a system to which you have no authority.

Herefordshire & Worcestershire CCG regularly monitor systems and unauthorised attempts at accessing systems may be investigated. Monitoring will be undertaken on behalf of the CCG by the commissioned IT Service Provider.

- All computer users are given a Username and Password; these are unique and must not be shared with anyone.
- Herefordshire & Worcestershire CCG employees or IT Service provider staff will never ask you to divulge your password.
- No user is permitted to log onto any other user's account - In the (unlikely) event that there is a requirement to access another user's account, the requester's line manager must support this request, along with approval via the relevant ELT lead. Approvals must be recorded through the IT Service Desk team who can grant access once authorised.
- Passwords should not be written down or kept where others might find them.
- Passwords should not be based on anything, which could be guessed easily by someone, obtained from social networking sites or personal information such as name, telephone number or date of birth.
- Your Herefordshire & Worcestershire CCG password must be different from that used on external or personal systems.
- Passwords should be complex, ensuring a combination of letters and digits of a pre-determined length and combination of characters
- Passwords may contain characters from each of the following categories:

- ✓ English Upper Case Letters: (A, B, C, Z, etc)
- ✓ English Lower Case Letters: (a, b, c, z, etc)
- ✓ Westernised Arabic Numerals (0, 1, 2, 9, etc)
- ✓ Special Characters (!, $, #, %, etc)

- Passwords must be changed upon suspicion or indication of compromise.
- Password history enforcement is in place to prevent passwords being re-used.
- Some systems might be configured to force password changes at regular intervals.

Requests to access applications must be logged via your IT Service Provider Service Desk and access will only be authorised if access is required for your work.

Your computer account for everyday business work will not have elevated rights which permit the installation of software or changes in configuration on Herefordshire & Worcestershire CCG computers. If administrative rights are required, a separate account will be created which must only be used for the intended task and the password must be different the non-elevated rights account password.

You or your manager must notify your IT Service Provider Service Desk of any change in role. You may not retain access to information or systems unrelated to your current employment.

You must not use your credentials or equipment when you are not employed by Herefordshire & Worcestershire CCG. All equipment, IDs and authentication tokens must be returned to your manager or their representative on the last day of employment or at the earliest opportunity.

5.3.3 Unattended Equipment

Computer equipment that is logged on and left unattended can present a tempting target and gives people access to systems you use. Unauthorised access of an unattended laptop/pc can result in harmful or fraudulent use.

Equipment should therefore always be safeguarded appropriately – especially when left unattended.

- You are required to lock or log out of your computer prior to leaving it unattended.
- Don’t wait for the screensaver

Windows Key  **+ L** Locks your computer

Displays the options to lock, logout or change your password

- Screen locks/savers must be password protected and may only be suspended whilst delivering presentations.

5.3.4 Maintenance

You must allow your IT Service Provider IT support staff (and authorised contractors) access to your Herefordshire & Worcestershire CCG computer when maintenance is required. Times will be arranged so that they are mutually convenient but scheduling of maintenance cannot be postponed indefinitely.

You must allow for the installation of updates on your computer. To do this efficiently updates are distributed using software. When prompted to install updates or a restart is required you will be given several opportunities to postpone, but these must take place at the earliest opportunity.

To keep end user devices in good order, it is advisable to re-start your device on a regular basis. Please ensure that the equipment you are provided with (laptops and PCs) are regularly re-started to maintain performance.

5.3.5 Portable IT Assets

Laptops, tablets, mobile phones, smartphones and other portable devices must not be left unattended. They must not be left in sight in cars, public transport or hotels. They should not be kept on desks overnight; they must be stored in locked cupboards/drawers or taken home. They must not be left in vehicles overnight.

Laptops, tablets, mobile phones, smartphones and other portable devices containing Herefordshire & Worcestershire CCG information must be encrypted to protect the information. You must not remove the encryption from these devices.

Only members of IT (or approved contractors) are permitted to move any non-portable IT equipment, whether within an office or to another site.

Loss of equipment must be reported as soon as possible to the IT Service Desk.

5.3.6 Use of Personal Computer Equipment

The use of personal devices for work is not generally permitted and requires authorisation from a member of Herefordshire & Worcestershire CCG's Executive Leadership Team.

Herefordshire & Worcestershire CCG sensitive information or personally identifiable information must not be held on equipment not owned and managed by Herefordshire & Worcestershire CCG.

No personal peripheral devices of any kind (digital cameras, smartphone, tablet, removable storage etc.) may be bought, installed or configured on any Herefordshire & Worcestershire CCG computer.

The use of privately owned equipment for remote access and usage whilst at work is covered in the relevant sections of this standard (5.3.7).

If you intend to use your own IT equipment to connect from home it will only provide specific application access (such as MS Teams, O365). You should maintain minimum security standards on your computer:

- Install the latest security fixes or updates.
- Use antivirus software.
- Use a personal firewall.
- Not be used by anyone else whilst accessing Herefordshire & Worcestershire CCG information or systems.

5.3.7 Working Remotely

Herefordshire & Worcestershire CCG employees must observe the points below when working away from the office.

This applies to your use of any Herefordshire & Worcestershire CCG communications facilities whenever you are working on business away from Herefordshire & Worcestershire CCG's premises.

Permission to use and connect to Herefordshire & Worcestershire CCG computing and communications devices or systems whilst away from our offices is at the discretion of your manager and controlled by Herefordshire & Worcestershire CCG and your IT Service Provider on behalf of the CCG.

You are responsible for ensuring the security of Herefordshire & Worcestershire CCG property including laptop equipment, screens, webcams, mobile phones, headsets and all Herefordshire & Worcestershire CCG information, files, documents, data etc. within your possession, including both paper and electronic material.

Whilst working from home the CCG's Information Security and Information Governance arrangements still apply and employees should ensure they are familiar with these policies.

You must take additional care when working with information and computing and communications devices or systems outside of our secure offices.

When you are working remotely, you must:

- Obtain authorisation before taking personal or sensitive information away from our offices;
- Not leave equipment and files unattended in public areas;

- Not use their own personal computer to work on personal identifiable data or sensitive corporate information;
- Position yourself so that your work cannot be overlooked by any other person;
- Ensure that sensitive information is not overheard, especially in public areas;
- Not load unauthorised software onto a CCG laptop or device without permission;
- Not discuss or show sensitive Herefordshire & Worcestershire CCG information to those with no right to know;
- Take reasonable precautions to safeguard the security of your laptop computers and any computer equipment on which you do Herefordshire & Worcestershire CCG business, locking equipment and sensitive information away or storing out of sight;
- Not download or save any CCG data to home storage devices or upload to cloud storage or backup services (such as, but not limited to, personal O365 accounts, Dropbox, Box, Google drive, Huddle, etc);
- Keep your passwords secret;
- Keep any 2-factor authentication method and PIN numbers private;
- Inform their Line Manager as soon as possible if records, equipment or any computer equipment on which you process Herefordshire & Worcestershire CCG work has been stolen;
- Ensure that any work which you do remotely is saved on Herefordshire & Worcestershire CCG's system or is transferred to Herefordshire & Worcestershire CCG's systems, as soon as is reasonably practicable;
- Ensure that ID badges, remote access tokens or memory sticks are kept separately from computer equipment when not in use;
- Seek advice from your Herefordshire and Worcestershire SIRO or IT Service Provider before taking any supplied IT equipment outside the United Kingdom or requirements to work whilst abroad. Transporting personal, sensitive or encrypted information outside of the UK may breach our legal obligations. The equipment may not be covered by our normal insurance against loss or theft and can be confiscated by Airport Security personnel.
- Ensure CCG issued equipment is not used by others i.e. family and friends, etc

Herefordshire & Worcestershire CCG reserve the right to check for these standards each time you connect with personal computing equipment and may deny the request if it does not meet our requirements.

It is your responsibility to check that the performance and reliability of your internet connection is adequate for working remotely and contact your internet service provider to resolve issues.

Homeworkers who are using Company supplied and supported equipment can receive telephone support from your IT Service Provider, but if the issue cannot be resolved by telephone, they will be required to bring the equipment to our offices, as home visits

are not possible. It is not possible for Herefordshire & Worcestershire CCG to provide support for equipment owned by members of staff.

Further information in relation to equipment available for home working and working safely at home, please see the Home Working Policy.

5.3.8 Removable Media

Removable media devices are those used to store and transport information and include, but are not restricted to the following:

CDs, DVDs and other optical disks	External Hard Drives
USB Memory Sticks (also known as pen drives or flash drives)	Memory or Media Cards (for example SD Memory Cards)
Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)	MP3/MP4 Players
Digital Cameras	Backup Tapes
Audio Tapes (including Dictaphones and Answering Machines)	

Storing sensitive information on removable media should be avoided. These devices must never be used for storing the main or only copy of important information.

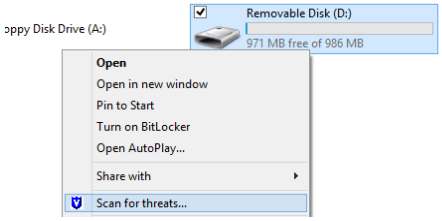
The use of removable media is a frequent cause of data protection breaches when personal identifiable information is lost, disposed of incorrectly or given to the wrong person.

The following applies to the use of any removable media:

- The information on removable media must always be protected by a password or PIN.
- If sensitive or personally identifiable information is on the device it must be encrypted.
- Herefordshire & Worcestershire CCG provides appropriate USB removeable storage devices which can be ordered through your IT Service Provider Procurement.
- Due to the size and portability of removable media special care must be taken to prevent loss or damage.
- You must report losses of removable media to your IT Service Desk and IG lead, especially when it involves personal or sensitive information.

- Removable media is a common route for transferring malicious software such as viruses, you must not use personal removable media devices to transfer files between your personal computer and Herefordshire & Worcestershire CCG.
- Removable Media must be scanned for malicious software before opening or transferring files:

Right Click and Select “Scan for Threats…..”



5.3.9 Disposal of Equipment

Disposal of IT equipment will be arranged by your IT Service Provider with due regard to security, legal (data protection and software compliance) and environmental issues, ensuring that the appropriate hardware and software registers are updated.

Any redundant, faulty or unused hardware or software must be returned to your IT Service Provider. This can be done by contacting the IT Service Desk.

All issued equipment must be returned at the end of employment.

Herefordshire & Worcestershire CCG does not permit the purchase of company owned equipment at the end of employment.

5.4 Telephones

The misuse of Herefordshire & Worcestershire CCG’s telephone services is also considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action.

Herefordshire & Worcestershire CCG provide desk, mobile and smart phones for the purpose of supporting its business.

You are not permitted to access the following services unless it is pertinent to fulfilling Herefordshire & Worcestershire CCG’s business obligations

- International telephone services.
- Premium rate services.
- Premium rate text services.

Personal use of telephone services is at the discretion of your manager.

5.4.1 Mobile Phones and Smartphones

Your Herefordshire & Worcestershire CCG mobile or smartphone must require a PIN or password to unlock.

You must not store sensitive Herefordshire & Worcestershire CCG or customer information or sensitive personally identifiable information on mobile phones or smartphones.

Our standard contract for your CCG mobile phone budgets for expected work use for mobile working. Mobile data is not unlimited and additional use above the capacity purchased will incur additional charges.

If your work requires frequent use of the Internet from your phone or high usage such as tethering your work smartphone to a Herefordshire & Worcestershire CCG computer you must consult with your manager and Procurement who will advise on the best options.

You must not tether your work smartphone to personal computer equipment to provide Internet access.

You must not use the Internet access via your phone for bandwidth intense applications such as watching television or films.

You must not use a corporately provided mobile phone for personal use (including personal photos, video, music, files, file sharing and apps for personal use).

You may not install applications or games onto your smartphone without authorisation.

It is your responsibility to ensure the safekeeping of any telecommunications equipment in your control. Any theft or loss must be reported to your line manager and the Service Desk immediately.

You must not use a mobile phone while driving any vehicle (driving means whenever the engine is switched on, even if the vehicle is stationary), unless using 'hands free' equipment. Even with this provision, conversations should be as brief as possible.

5.4.2 If your phone is faulty, lost or stolen

Procedures for faulty phone

- Inform your line manager
- For Herefordshire:
    - You need to call EE on 158 direct from an EE mobile phone, or 07973 100158 from any other phone.
    - Contact ICT service desk to log an incident for replacement device.
- For Worcestershire:
    - Contact the Senior Corporate Services Officer who will liaise with O2 and arrange a repair/replacement device.

Procedures for lost or stolen phones

You need to:

- Advise your manager.
- Advise the Service Desk. If your phone has been configured to pick up Herefordshire & Worcestershire CCG e-mail then we need to remotely wipe the device.
- Report the event to the relevant police station by the user within 24 hours of discovering the loss. The police will issue you with a reference number.
- For Herefordshire:
    - Call EE on 158 direct from an EE mobile phone, or 07973 100158 from any other phone to request the phone is barred and blacklisted. They will require the police reference number from you and a full description of the event leading to the loss/theft.
    - Request quotation from ICT Procurement if a replacement device is required

    Further support, ordering and account authorisation can be obtained by contacting the ICT Service Desk on 01432 260160 or via the ICT Service Desk Icon on your Herefordshire & Worcestershire CCG PC / Laptop.
- For Worcestershire:
    - Contact the Senior Corporate Services Officer who will liaise with O2 and arrange for the phone to be barred and blacklisted and for a replacement device to be issued.

5.4.3 Use of Personal Phones

Using your own phone at work whether it is for calls, texting, internet access, e-mail or other application should be limited to breaks and outside of working hours.

It is understood that on occasion it is necessary to make or receive important personal calls and text messages during work. If this is going to happen consistently permission must be sought from your manager.

Unjustified frequent personal calls, checking of personal e-mails, social networking or texting during work hours is unprofessional and inappropriate. If your manager feels that this is causing a problem you will be subject to performance management/disciplinary procedures.

You must not connect your personal phone to Herefordshire & Worcestershire CCG equipment or the corporate network.

5.4.4 Use of Voicemail

You must not leave sensitive information on voice mail or answerphone messages.

You must not attempt to access the voicemail of another person without prior authorisation.

Authorisation for accessing another person's voicemail without their consent must come from a member of Herefordshire & Worcestershire CCG's Executive Leadership Team.

5.5 E-mail

E-mail is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, or that the content will be understood in the way that the sender of the e-mail intended. It is therefore the responsibility of the person sending an e-mail to decide whether e-mail is the most appropriate method for conveying time critical or sensitive information or of communicating in the particular circumstances.

Copies of e-mails can be used in investigations, employee tribunals, Subject Access Requests and Freedom of Information Requests.

Always check the address of the recipient, take extra care if sending sensitive information making sure that the e-mail address is correct for the content.

Please check all your messages carefully before sending them, making sure they are accurate and the tone is appropriate. If you have any concerns, please speak to your line manager first. All outgoing e-mails bear Herefordshire & Worcestershire CCG's name, care should be taken not to contain any material which would reflect poorly on Herefordshire & Worcestershire CCG or the NHS's reputation or adversely affect its relationship with existing and potential providers, clients or business partners.

5.5.1 E-mail Addresses

E-mails that are used to conduct business on behalf of Herefordshire & Worcestershire CCG may be sent from e-mail addresses with the following suffixes:

Firstname.lastname@nhs.net - Standard address used for Herefordshire & Worcestershire CCG Employees and Contractors

Where there is more than one account already with the same name, the next available numbered address will be chosen and allocated to the user. For example: firstname.lastname3@nhs.net.

5.5.2 E-mail Signature

E-mails must have a signature configured by individual account holders and a disclaimer which will be automatically stamped to all external messages by the mail server.

Your signature must conform to Herefordshire and Worcestershire brand guidelines to be found on The Hub, under Templates.

Your e-mail signature should not include any personal messages such as sponsorship and personal qualifications.

NHS.net automatically inserts an email ‘disclaimer’ at the footer of every email sent, which is a nationally set NHS disclaimer.

5.5.3 E-mail Usage

Herefordshire & Worcestershire CCG e-mail accounts must not be set up to automatically forward messages to non-Herefordshire & Worcestershire CCG e-mail accounts. Remote access to emails is possible with Herefordshire & Worcestershire CCG Smartphone or remote access. It is also possible utilising personally owned devices – however the functionality will be limited when not utilising an NHS device.

When sending emails containing PCD or commercially sensitive information, the email must be sent to and from an nhs.net account, or other nhs.net compatible account such as:

- Gov.uk
- Secure.nhs.uk
- Gov.uk
- Cjsm.net
- Pnn.police.uk
- Mod.uk
- Parliament.uk

When sharing sensitive information with non-accredited or non-secure email services, such as those ending in .nhs.uk, Hotmail Gmail and Yahoo, the NHSMail encryption facility must be used. Guidance on how to use this can be found at https://portal.nhs.net/Help/policyandguidance

The transmission of any sensitive corporate information to private e-mail addresses is strictly prohibited and staff should note will be subject to our disciplinary procedures.

If you receive an e-mail which is intended for another person and is not marketing, spam or junk, you must delete the e-mail immediately from the inbox and “Deleted Items” and notify the sender. If the e-mail contains confidential information you must not make use of it or disclose it to anyone else.

You must not access another user’s e-mail without authorisation.

If there is a requirement for others to access your e-mail, for example at the end of your employment or for PA/admin support, you should use the properties of your Inbox to assign the required permissions to your inbox as required.

You must not impersonate any other user when using e-mail or amend the content of any message received unless specifically authorised.

E-mail must not be used for:

- The transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.

- The unauthorised transmission to a third party of OFFICIAL or OFFICIAL-SENSITIVE material concerning the activities of the Herefordshire & Worcestershire CCG or its partners/providers.
- The unauthorised transmission to personal email account or personal file storage (such as but not limited to personal O365, Dropbox, Huddle, etc) of OFFICIAL or OFFICIAL-SENSITIVE material concerning the activities of the Herefordshire & Worcestershire CCG or its partners/providers.
- The transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- Activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- The creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- The creation or transmission of material that is abusive or threatening to others or serves to harass or bully others.
- The creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- The creation or transmission of defamatory material.
- The creation or transmission of material that includes false claims of a deceptive nature.
- So-called ‘flaming’ - i.e. the use of impolite terms or language, including offensive or condescending terms.
- Forwarding chain letter e-mails.
- Activities that violate the privacy of other users.
- Unfairly criticising individuals, including copy distribution to other individuals.
- Publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- The creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- The creation or transmission of material which brings Herefordshire & Worcestershire CCG or its customers into disrepute.

5.5.4 E-mail Security Threats

Common threats to security which are specific to e-mail are:

- Junk E-mail and Spam.
- Phishing or a scam sent en masse to try and net responders, passwords or financial information.
- Spear Phishing or Whaling attacks (Uses public information to make the message appear authentic)
- Distribution of Malicious Software.

If you receive a spam or phishing message in your NHS mail inbox it's important that you report it to the NHSmail help desk for analysis and monitoring. Forward the email as an attachment to spamreports@nhs.net

To guard against e-mail threats:

- Do not use Herefordshire & Worcestershire CCG e-mail addresses for personal use.
- Opt out of marketing if you must register your business e-mail.
- Be suspicious, if it is too good to be true …..it probably is!
- Do not disclose bank account details, passwords or payment details via email
- Never open or reply to junk or spam.
- Never send your passwords or financial information.
- Never install software sent via e-mail.
- Never open attachments from suspicious e-mails.
- Never follow links in suspicious messages.
- Hover over links to see the true address.

If you suspect you have received an e-mail containing a virus you must immediately contact the Service Desk. Do not forward the suspected e-mail to anyone.

5.5.5 E-mail Restrictions and Maintenance

E-mail messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed 25mb in size.

Your e-mail must not be used as a document store. If a record is required, important communications and files must be transferred to the appropriate network file location or system.

Regularly delete old e-mails, particularly those with file attachments.

5.5.6 Monitoring of E-mail

Whilst respecting the privacy of authorised users, Herefordshire & Worcestershire CCG maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of e-mail by authorised users to ensure adherence to its policies and standards.

All use of NHS mail is subject to the policies and acceptable use policies of NHS mail which be found at: https://digital.nhs.uk/services/nhsmail/nhsmail-policies

Any interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from our systems.

It should also be noted that e-mail and attachments may need to be disclosed under current data protection legislation or the Freedom of Information Act 2000.

All users should be aware that e-mail usage is monitored by the NHS Mail service and recorded centrally. The monitoring of e-mail (outgoing and incoming) traffic will be undertaken so that NHS Mail can:

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.

Archives and retention of NHS Mail are as per the NHS mail policies and procedures found here: https://digital.nhs.uk/services/nhsmail/nhsmail-policies

Monitoring of content will only be undertaken by staff specifically authorised for that purpose. These arrangements will be applied to all users and may include checking the contents of e-mail messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of e-mail facilities.
- Ensuring effective operation of e-mail facilities.
- Determining if communications are relevant to the business.

Where a manager suspects that the e-mail facilities are being abused by a user, they should contact follow the NHS Mail Access to Data procedure found here: https://support.nhs.net/knowledge-base/nhsmail-access-to-data-procedure/

Access to another person's e-mail is strictly forbidden unless that person has given their consent, or their e-mail needs to be accessed by their line manager for specific work purposes such as they are absent from work and access is required to deal with any business communications or they no longer work for Herefordshire & Worcestershire CCG. If this is the case a member of Herefordshire & Worcestershire CCG's Executive Management Team must authorise the request. This must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the individual. Managers must only open e-mails which are relevant.

5.6 Network Security

All staff should be vigilant to avoid unauthorised personnel trying to connect to the NHS HSCN network and any services or data belonging to Herefordshire & Worcestershire CCG on that network. HSCN is a secure network which connects NHS organisations and must maintain compliance to national standards in order to retain connections to health and government networks.

Personal or unauthorised networking equipment such as switches, hubs or wireless access points must not be connected to the network.

Access to network infrastructure equipment must be restricted to employees of Herefordshire & Worcestershire CCG IT and authorised contractors or suppliers.

5.6.1 Third Party/Supplier Network Access

Herefordshire & Worcestershire CCG's IT Service provider must be informed and authorise new services or contracts that requires third parties (those not a current member of staff of Herefordshire & Worcestershire CCG) having access to our internal network or infrastructure.

You are to ensure that third parties including consultants and contractors do not plug their computers onto our network without prior approval. Any non-Herefordshire &

Worcestershire CCG employees should make use of the Patient Wi-Fi network or Guest Wi-Fi (dependent on site and availability).

Any supplier access required should be organised via your IT Services Provider and should only permitted if approved by your IT Service Provider.

Changes to computing and communications devices or systems which Herefordshire & Worcestershire CCG is responsible for must be controlled so that they are aligned to Herefordshire & Worcestershire CCG's requirements and do not adversely impact information security. Changes to IT systems must be processed through your IT Services Provider and signed off by your Director of Digital Strategy and Infrastructure or nominated deputy.

5.7 Internet Access

Access to the internet is provided to support Herefordshire & Worcestershire CCG's business.

5.7.1 Personal Use of Internet Access

Use of the internet for personal use is at the discretion of the organisation and is permitted so long as this does not interfere with work, your work environment or your productivity at work, and if it does not breach locally defined policies, procedures and complies with 'Internet safe usage' outlined below.

If demands at particular times of the day become excessive (e.g. lunchtime) and performance of the network suffers as a result, personal access may have to be reduced or removed.

You should be aware that your personal use of the internet via your work equipment is filtered and monitored as described in this standard.

Herefordshire & Worcestershire CCG is not responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep Herefordshire & Worcestershire CCG protected against any claims, damages, losses or the like which might arise from your transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via Herefordshire & Worcestershire CCG's Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of Herefordshire & Worcestershire CCG.

If you wish to register as a user of a website for non-work purposes you must not give your own or any colleague's work e-mail address for personal transactions or communications.

You must never download any software or copyrighted material from the internet for personal use.

If you are in any doubt about how you may make personal use of the Herefordshire & Worcestershire CCG's Internet service you are advised not to do so.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Herefordshire & Worcestershire CCG and may be accessed at any time by the Herefordshire & Worcestershire CCG or it's IT Service Provider to ensure compliance with all its statutory, regulatory and internal policy requirements.

5.7.2 Internet Safe Usage

You must be aware that information sourced from the internet may be incorrect and that its authenticity and bias should be verified if used for business purposes.

You must not use internet access for any improper, immoral, fraudulent or unlawful purposes or to access, store, create or transmit any material which is offensive, abusive, indecent, defamatory, obscene, or menacing. For example sexually explicit material or offensive content based upon race, sex, sexuality, disability, age or religion.

You must not:

- Store sensitive Herefordshire & Worcestershire CCG, customer or personally identifiable information on internet file sharing and e-mail sites including, but not limited to: Box, DropBox, Hotmail, Google's Drive or Gmail.
- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Unless required as part of your work, stream live or on demand media content such as television, film or music.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise non-business related real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gambling or betting sites.
- Subscribe to, enter or use online computer gaming sites or browser based games.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Distribute or use copyrighted material without permission of the owner.
- Use work internet or equipment to run a private or free-lance business.
- Download any software which is not distributed or authorised by Herefordshire & Worcestershire CCG.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the

rules, essence and spirit of this and other Herefordshire & Worcestershire CCG policies.

5.7.3 Internet Filtering

Herefordshire & Worcestershire CCG and its IT Service provider uses software to monitor internet access, screen out harmful webpages and apply the content restrictions described in this policy.

You must not use techniques to bypass filtering, anonymise or disguise your internet usage. Installation of software or using an external service to do this will result in disciplinary action.

The download of executable files from websites is blocked and where appropriate Herefordshire & Worcestershire CCG may also block individual websites or pages.

Requests to unblock a site must be raised with your IT Service Provider via their IT Service Desk.

If the requirements of your work require access to a category of site normally blocked, your Line Manager must authorise the request.

5.7.4 Internet Monitoring

Your access to the internet using Herefordshire & Worcestershire CCG computers or network is monitored. Please bear in mind that you may be called upon to justify the amount of time you have spent on the Internet or the sites you have visited.

Some of the details recorded are:

- The name of the account making the request.
- The address of the computer from which the request was made.
- The webpage address requested.
- The category of site visited.
- Whether the request was permitted or blocked.
- Whether the site is associated with productivity loss.
- The number of requests for each website or page.
- An estimate of the time spent on each website or page.

Herefordshire & Worcestershire CCG may periodically run reports to identify breaches in policy or standards.

Managers may request internet activity reports for the individual in their service area by contacting the Service Desk.

5.8 Social Media

All staff must adhere to the guidance below in relation to the use of Social Media.

You remain accountable for your actions, views and opinions irrespective of whether the computing and communications devices or systems is provided by Herefordshire & Worcestershire CCG or privately sourced. Actions, views and opinions which damage the reputations of Herefordshire & Worcestershire CCG or its customers must not be made.

5.8.1 Participating in on-line activities

Our staff are our best ambassadors. Many already use social media, interactive and collaborative websites and tools, both in a personal and professional capacity. Rather than try to restrict this activity, Herefordshire & Worcestershire CCG wish for staff to interact online in a way that is safe, responsible, credible, consistent, transparent and relevant.

We recognise that there is an increasingly blurred line between what was previously considered 'corporate social networking', which could be useful to the business, and 'social networking', which is for personal use, to an extent where it may no longer be possible, or desirable, to make that distinction. For example, there is a tendency for people to maintain just one Twitter account, which is used to post a mixture of business related and personal content.

However, posts made through personal accounts that are public can be seen and may breach organisational policy if they bring the organisation into disrepute. This includes situations when you could be identifiable as a Herefordshire & Worcestershire CCG employee whilst using social networking tools or occasions when you may be commenting on Herefordshire & Worcestershire CCG related matters in a public forum.

Staff should use their own discretion and common sense when engaging in online communication. The following guidance gives some general rules and best practices which you should abide by at all times:

- Know and follow Herefordshire & Worcestershire CCG's codes of conduct and information security policies (which can be found on the staff intranet). The same principles and guidelines that apply to staff activities in general also apply to online activities. This includes forms of online publishing and discussion, including blogs, wikis, file-sharing, user-generated video and audio, virtual worlds and social networks.
- Employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media. Be mindful that what you publish will be public for a long time. When online, use the same principles and standards that you would apply to communicating in other media with people you do not know. If you wouldn’t say something in an email or formal letter, don’t say it online and do not, under any circumstances, bring your employer into disrepute by your comments or actions on social media.

- Identify yourself by giving your name and, when relevant, role at Herefordshire & Worcestershire CCG if you are discussing Herefordshire & Worcestershire CCG related matters. Write in the first person. You must make it clear that you are speaking for yourself and not on behalf of Herefordshire & Worcestershire CCG (you must not use the organisation's logo on personal web pages or social media accounts).
- Be aware that people who join your networks and participate in groups that you are a member of may be colleagues, clients, journalists or suppliers. It is also possible that people may not be who they say they are and you should bear this in mind when participating in online activities.
- If you publish content to any website outside of Herefordshire & Worcestershire CCG that could be perceived to have a connection to the work you do or subjects associated with Herefordshire & Worcestershire CCG, you must display a disclaimer such as this: "My postings on this site reflect my personal views and don't necessarily represent the positions, strategies or opinions of Herefordshire & Worcestershire CCG."
- Respect copyright, fair use, data protection, defamation, libel and financial disclosure laws.
- Don't reveal confidential information about patients, staff, or the organisation.
- Never post any information that can be used to identify a patient's identity or health condition in any way.
- Don't use social media in any way to attack or abuse colleagues or members of the public.
- Don't provide Herefordshire & Worcestershire CCG's or another's confidential or other proprietary information on external websites.
- Do not publish or report on conversations that are private or internal to Herefordshire & Worcestershire CCG (for example, do not quote such material in a discussion forum post).
- Don't cite or reference partners or suppliers.
- Respect your audience. Don't use personal insults, obscenities, 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 Herefordshire & Worcestershire CCG when using online social networks. If you identify yourself, or are identifiable, as an employee of the organisation, ensure your profile and related content is consistent with how you wish to present yourself to colleagues and stakeholders.
- Be aware that you may be identified as an employee by any public use of your NHSmail email address.
- If you are asked to blog or participate in a social network for commercial or personal gain, then this could constitute a conflict of interest.

- You should refrain from entering any online social networking activity for commercial gain.
- If someone from the media contacts you about posts you have made, you must not engage in any communication without first checking if this permitted via your CCG Communications team.
- Don't pick fights, be the first to correct your own mistakes, and don't change previous posts without indicating that you have done so.
- Don’t use social media to “whistleblow” without already having raised concerns through the proper channels. All staff should be aware that the Public Interest Disclosure Act 1998 gives legal protection to employees who wish to whistleblow any concerns
- If you have any concerns about your position on any of the issues covered by this policy please contact the Digital Team or HR

Note that use of Herefordshire & Worcestershire CCG equipment and networks to participate in social media activities during your own time is covered by the Internet Usage requirements (Section 5.7).

5.8.2 Safeguarding

During the course of your work for Herefordshire & Worcestershire CCG you may have cause to engage in online conversations with, and the promotion of, engagement opportunities with children, young people and adults at risk. The use of social media/networking sites introduces a range of potential safeguarding risks to these groups.

Most children, young people and adults use the internet positively, but sometimes they and others may behave in ways that pose a risk. Potential risks can include, but are not limited to:

- Online bullying
- Grooming, exploitation or stalking
- Exposure to inappropriate material or hateful language
- The vulnerable person giving away personal details, which can be used to locate them, harass them or steal their identity
- Coercion into illegal activity, such as distributing illegal content or hate crime
- Indoctrination into ideations and encouraged into terrorist activities
- Encouraging violent behaviour, self-harm or risk taking
- People's wellbeing not being promoted, as their views, wishes, feelings and beliefs are not taken into account.

In order to mitigate these risks there are steps you can take to promote safety online:

- Don't target/or engage with children who are likely to be under the minimum requirement age for the social networking service that you are promoting. This is usually 13 years, but can vary by platform so check the T&Cs of that site.
- Don't accept 'friend' requests from anyone you suspect to be underage.

- Avoid collecting, and don't ask users to divulge any personal details, including: home and email addresses, school information, home or mobile numbers.
- You should not use any information in an attempt to locate and or meet a child, young person or vulnerable adult, that is not directly to do with work.
- The Sexual Offences Act (2003) combat increasing sexual approaches to access children and young people on-line. The Act 2003 created an offence of meeting a child following sexual grooming. This makes it a crime to befriend a child on the Internet or by other social media means and to arrange to meet or intend to meet the child or young person with the intention of abusing them.
- Be careful how you use images of children, young people or adults - photographs and videos can be used to identify them to people who wish to groom them for abuse.
- consider using models, stock photography or illustrations. Therefore work with your Communications team if you need to use any images of children in relation to your work.
- Ensure that any messages, photos, videos or information comply with existing policies.
- Promote safe and responsible use of social media/networking to your audience online and consider providing links to safety and support organisations on your profile. Remind people to protect their privacy.
- Data Protection considerations - when you are collecting personal information about all users, you should always follow the requirements set out in the Data Protection Act 2018. You should not use social media to collect personal data and this should be done via alternative means, e.g. by signposting to a form on your website.

5.8.3 Safeguarding yourself

In addition to the behaviours outlined in sections above, if you are using corporate or personal social media/networking accounts for work related activity, you should also:

- Ensure that your privacy settings are set up so that personal information you many not want to share is not available to members of the public.
- Have a neutral picture of yourself as your profile image.
- Do not use your work contact details (email or telephone) as part of your personal profile or personal contact details as part of a profile you use for work.
- Keep yourself safe, if you are not sure then do not proceed without advice and support.
- Do not engage in intimate or sexual conversations.
- Ensure any personal pictures you upload are not intimate, compromising or sexually explicit.
- Should any employee encounter a situation whilst using social media that threatens to become antagonistic they should politely disengage and seek advice from the Communications Team and/or their line manager.

5.8.4 Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to your local safeguarding lead within Herefordshire & Worcestershire CCG.
- With regard to personal safeguarding, you should report any harassment or abuse you receive online whilst using corporate or personal accounts for Herefordshire & Worcestershire CCG related business, to the Communications Team in the first instance They will advise you what further action should be taken and escalate to Herefordshire & Worcestershire CCG's legal, security and HR teams as required.
- Keep yourself and others safe. Do not place yourself at risk and engage in risk taking behaviour on social media platforms.

5.8.5 Personal blogs

If you are writing a personal blog, you should adhere to the guidance given in section 5.8.1 if your blog touches on any work-related matters. You must also include a disclaimer which says:
"Any views expressed in this blog are entirely my own and not those of my employer."

5.8.6 References and endorsements

For social networking sites such as LinkedIn where personal and professional references are the focus: If you are representing yourself as a Herefordshire & Worcestershire CCG employee, you may not provide professional references about any current or former employee, contactor, vendor or contingent worker. You may provide a personal reference or recommendation for current or former Herefordshire & Worcestershire CCG employees, contractors, vendors and contingent workers provided:
the statements made and information provided in the reference are factually accurate; and you include the disclaimer below:
"This reference is being made by me in a personal capacity. It is not intended and should not be construed as a reference from Herefordshire & Worcestershire CCG."

5.8.7 Responding to the media

As an organisation, we do not encourage staff to engage in "unofficial", spontaneous exchanges in response to published media comment e.g. Pulse, The Guardian or less traditional forms of journalistic content e.g. blogs, responses to online newspaper articles. If you intend to do so, then you must identify yourself as a Herefordshire & Worcestershire CCG employee and make it clear that you are speaking for yourself. Wherever possible include the following disclaimer:
"These views are entirely my own and not necessarily those of my employer."

When acting in your official capacity as an employee, on behalf of Herefordshire & Worcestershire CCG, you must not engage in responding to content published by third parties by adding comments.

If you read something online that you feel is factually incorrect, inaccurate or otherwise needs an official response from Herefordshire & Worcestershire CCG, then you must refer the matter to the Communications Team who will decide if a response is required.

5.8.8 Representing Herefordshire & Worcestershire CCG online

Whilst we encourage individual members of staff to use social media to reflect positively on the work of Herefordshire & Worcestershire CCG, it is important that the organisation maintains a coherent online presence through the strategic use of official communication channels. Therefore, without having developed a business case, and gained approval from the Communications Team and Executive Leadership team, you must not engage in setting up

- Twitter accounts, Facebook pages, Instagram account, YouTube channels or a presence on any other social media site that seek to represent the official views of Herefordshire & Worcestershire CCG;
- unauthorised 'official' blogs on behalf of Herefordshire & Worcestershire CCG programmes or individuals; or,
- posting video content or setting up surveys using any unapproved online channels

5.8.9 Official presence on social media sites and blogs

Using social networking sites to communicate with stakeholders in a professional capacity is in many cases entirely appropriate. However, it is important that the time and effort staff spend on them is justified by the value to the business, and that the inherent risks are considered before this type of media is used. Social networking platforms can offer many opportunities to reach a specific audience but there are also potential pitfalls which staff must be careful to avoid.

If you wish to establish a Herefordshire & Worcestershire CCG presence on Twitter, Facebook, LinkedIn or any other social networking site, this must be approved by the Communications Team. The Communications team will provide advice and guidance on the acceptable use and management of any corporate social media accounts.

The Communications Team monitor all CCG social media accounts and mentions for any corporate social media accounts, to ensure that it is appropriate and in-line with the organisation's social media strategy.

5.8.10 On-line surveys

If you wish to run an externally facing online survey please contact the Communications Team for permission and support. The communications team have established methods and software with which to perform such activities and will provide you with advice and guidance on how to achieve this.

5.8.11 Participation in collaborative communities of practice

If you wish to participate in online collaboration using externally facing web-based tools, with NHS colleagues or suppliers, on Herefordshire & Worcestershire CCG

projects and documents, you must carefully consider security. In the majority of cases, when involved in collaborative working, discussion and the sharing of work-related information and documents must take place in a closed environment, behind a secure login, to minimise the risk of unapproved or commercially sensitive material reaching the public domain.

All information stored on internal or external websites must be held in accordance with the Herefordshire & Worcestershire CCG Information Governance Policies.

If you have a requirement to set up a new collaboration, community of practice or consultation space, you must contact the Communications Team to discuss your needs in the first instance. They will be able to advise on the tools and services available to fit your requirements.

5.9 Software Copyright Compliance

Under the Copyright law, which governs the use of intellectual property, including software, it is illegal to copy or distribute a piece of software unless expressly permitted by the copyright holder.

Herefordshire & Worcestershire CCG computers are regularly audited for software compliance.

If caught using illegal copies of software, Herefordshire & Worcestershire CCG may face not only a civil suit, but also company directors and individuals may also be charged with criminal liability.

Should such a prosecution be brought, the effects and costs relating to both the prosecution and adverse PR are immeasurable. User Responsibilities:

- You must not make or distribute any unauthorised copies of any software under any circumstance.
- You must not give any Herefordshire & Worcestershire CCG provided software to any third party, including clients and customers.
- All software must be purchased through Herefordshire & Worcestershire CCG procurement and distributed by Herefordshire & Worcestershire CCG IT Service provider, who will load the programs on the relevant computers or servers. This includes any upgrades to existing applications.
- If you determine that there may be a misuse of software within Herefordshire & Worcestershire CCG you must notify the IT Service Desk immediately.
- You are not permitted to bring software from home, and load it onto any of our computers.
- The loading of third party applications, games, wallpapers and screen savers on any Herefordshire & Worcestershire CCG computer is prohibited.
- Herefordshire & Worcestershire CCG software should not be taken home and loaded onto a user's home computer. If a user has to use software at home for Herefordshire & Worcestershire CCG's business, and is not provided with a Herefordshire & Worcestershire CCG computer for this purpose, a separate copy

of the software will be bought for the home computer, given that the appropriate authorisation has been obtained.

- The use of registered Freeware and Shareware may be permitted for appropriate business purposes only, provided it is licensed for business use, authorised, sourced and loaded by Herefordshire & Worcestershire CCG IT Service Provider.
- All software, information and programmes developed for and/or on behalf of Herefordshire & Worcestershire CCG by employees or contractors during the course of their employment remain the property of Herefordshire & Worcestershire CCG. Duplication or sale of such software without the prior consent of Herefordshire & Worcestershire CCG will be an infringement of our copyright and will be dealt with as a disciplinary matter.
- Non-work related audio, animation or video files are not to be downloaded. This includes, but is not restricted to mp3, mp4, avi, mpeg and mov files.

5.10 Antivirus

All Herefordshire & Worcestershire CCG computers have anti-virus software installed and scheduled to run updates at regular intervals.

You must report any viruses suspected or found on your computer to the IT Service Desk. If a virus is discovered on a computer, Herefordshire & Worcestershire CCG IT will remove the machine from the network and subject it to Herefordshire & Worcestershire CCG's malicious software handling procedure.

You should never download files from unknown or suspicious sources. All spam e-mails should be deleted and unknown or suspicious attachments must not be opened.

Never forward any spam e-mail or email you suspect may contain a virus.

You should never attempt to disable the anti-virus software. If problems arise, the user should contact the IT Service Desk for assistance.

Any attempts by you to create and/or distribute malicious programs into the Herefordshire & Worcestershire CCG managed network (such as viruses, e-mail-bombs, worms, Trojans etc.) are prohibited. Any user who engages in such activity will be subject to disciplinary and/or legal action.

5.11 Information Security Incidents

Employees should refer to the IG Handbook section on Data Security and Protection Incidents for details of the procedures to be followed for reporting information security incidents.

6. Compliance

Failure to follow the procedures described in this document may impact on good employee relations and the reputation of Herefordshire & Worcestershire CCG. Appropriate action (including disciplinary) will be taken if there is a breach in policy.

Contractors, agency workers and other individuals contracted to work for Herefordshire & Worcestershire CCG may have their contracts terminated without notice and incur financial penalties.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

7. Review and Revision

This standard will be reviewed as it is deemed appropriate, but no less frequently than every 36 months.

Policy and procedure review will be undertaken by the Herefordshire & Worcestershire CCG Corporate IT Group and Information Governance Group.

8. Linked Documents

Corporate Information Security Policy

Information Governance Management Framework

Information Governance/Data Security and Protection Policies

Information Governance Handbook