Herefordshire Council

Information Security Policy 2025 – 2028

Reference number	
Approved by	Information Governance Steering Group
Date approved	26 June 2025
Version *Last revised*	1.6 February 2025
Review date	March 2028
Category	Corporate Governance
Owner	Information Governance Manager
Target audience	All employees and members of the public.

After the Review Date has expired, this document may not be up to date. Please contact the document owner to check the status after the Review Date shown above.

This procedure may be reviewed earlier than the Review Date in the event of significant developments requiring changes to the document.

If you would like help to understand this document, or would like it in another format or language, please contact the document owner.

1.Introduction

Information is one of Herefordshire Council's most valuable assets and under data protection legislation we must ensure that information is processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Preserving the confidentiality, integrity and availability of the information in our care is essential to maintain our position as a respected and trusted organisation. The council has technical and organisational measures in place to protect data against accidental or unlawful destruction, or accidental loss or alteration and unauthorised disclosure or access. In particular, the council takes measures that are intended to ensure that:

- Anyone managing and handling data understands that they are contractually responsible for following good data protection practices.
- Everyone managing and handling personal data is appropriately trained to do so.
- Everyone managing and handling personal data is appropriately supervised.

Herefordshire Council holds structured and unstructured information electronically both on premises and hosted in cloud IT systems and physically in paper records; all of which must be suitably protected.

2. Purpose

This policy confirms Herefordshire Council's commitment to the continuous improvement of Information Security and highlights the key areas and controls in place to effectively secure information in our care. In particular:

- The requirements and activities outlined in this policy form part of the mitigation to reduce the risk to data security.
- It provides the framework for setting continuous information security objectives.

3. Scope

This policy applies to all staff (full time and temporary), councillors, contractors, suppliers and partners. For the purposes of this policy these groups will be referred to as 'colleagues'.

This policy is the minimum standard which should be applied whenever colleagues' access council facilities and equipment; in addition, local procedures, standards and work accompany this policy.

4. Responsibilities & Commitment

Herefordshire Council's Corporate Leadership Team and Information Governance Steering Group are committed to ensuring that all aspects of information security are complied with.

All colleagues have a role to play and a contribution to make to the safe and secure use of information and the technology used to manage it. All colleagues must work in accordance with all policies and procedures which includes information security specific requirements. Managers are responsible for ensuring that all new employees (permanent and temporary) complete their Induction along with the Information Security and Information Governance mandatory training modules on their first day of employment and before being provided with access to the council's Key Business Systems and Records. The modules must also be completed on an annual basis as a refresher, and if not could ultimately lead to withdrawal of access and disciplinary action.

Regular security training will be mandatory for all employees to ensure they are familiar with the council's security policies and practices. Targeted training will be provided to employees who manage sensitive information or perform critical security related roles.

If any user is found to have breaches this policy, they may be subject to disciplinary action. 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 in the first instance.

5. Keeping information secure

5.1 Protective Marking

Consideration must be given to protectively marking all written material in accordance with the sensitivity of its content.

The protective marking used by Herefordshire Council is:

OFFICIAL – Information where recipients must be mindful of data sensitivity.

OFFICIAL SENSITIVE – Information that could have damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. For example, personal information, sensitive personal information and commercially sensitive information.

Relevant sub-categories should also be used when available.

It will be assumed that any document not protectively marked contains unclassified information and we would be happy for it to be released into the public domain.

The Protective Marking of a document is applied by the originator (or in most cases the creator) and may only be changed with the originator's authority unless information becomes sensitive within exchanges (e.g. via email); or a contributor considers the original information should be marked as OFFICAL SENSITIVE.

'Private' or 'Confidential' are warning labels intended to inform recipients and do not form part of protective marking. Legal privilege can be used in relevant circumstances.

All information produced by the council is subject to the Freedom of Information Act (FOIA), Environmental Information Regulations (EIR) and Subject Access Requests (SARs) with or without protective markings.

Further information about how to apply protective markings can be found in the protective marking procedure.

5.2 Printing and Clear Desk / Clear Screen

For information security, cost and environmental reasons documents should not be printed unless it is absolutely necessary. If you do use printing facilities in an office, it is your responsibility to ensure that information is securely managed through storage or disposal and that all documents have been collected from printers.

Users are not permitted to have the facility to print documents to a non-corporate printer when working remotely.

Herefordshire Council has a clear desk policy in order to ensure that all information is held securely at all times. Documents must not be left unattended on desks or in meeting rooms and doing so will constitute a data breach. Hard copy information should be locked away when not in use and only disposed of within the secure waste bins located within council properties when no longer required. This applied when working in the office, at home or in a shared space accessed by others.

Storage is digital first (including scanning). Only where there is a legal requirement are paper files retained, with sensitive information locked away in appropriate storage when not in use, whether working in an office or at home.

To prevent inappropriate sharing of electronic information, colleagues must lock their screen when leaving their computer unattended.

5.3 Passwords

Passwords are the first line of defence of our ICT systems, and together with the user ID help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems. Staff need to have a unique password for access to Herefordshire Council systems which is not used for other purposes outside of work.

Users are required to adhere to Herefordshire Council's best practice regarding the use of secret authentication information. This includes the following requirements:

- Passwords must not be written down under any circumstances.
- Passwords must not be shared, except with an ICT representative and only following an approved process.
- Administrators must securely communicate passwords to users using approved secure channels.
- System access must be revoked promptly following the termination of employment, where doing so does not compromise the ongoing business operations of Herefordshire Council.

When creating or changing your Herefordshire Council password, you must use a complex password, a passphrase combining 3 random words and at least 2 special characters, which will enhance memorability while maintaining strong security.

Passwords must be:

- At least 15 characters long.
- Changed on indication or suspicion of compromise.

Password length and complexity requirements are as follows:

- Password (recommended 3 random word passphrase) using upper- and lower-case letters e.g. PaperHumbleConnect.
- Digits (0-9) e.g. PaperHumbleConnect8
- Special characters, such as: `'-!"#$%&()*,./:;?@[]^_{|}~+<=>` e.g. PaperHumbleConnect9#!

  Please note that currency symbols like € or £ are not considered special characters.

Passwords must not:

- Contact your login ID.
- Include 3 or more consecutive characters from your full name.
- Be based on anything which could be easily guessed by someone or obtained from personal information such as name, telephone number or date of birth.
- Contact a well-known phrase, like a saying from a film or book such as “Hasta la vista” or “to be or not to be”.

Hoople IT periodically audits the robustness of user passwords using password-cracking software.

5.4 Working away from the office

All staff have the ability to connect to the council network whilst working away from an office location i.e. working from home or a remote location. Staff are however advised that public Wi-Fi connections are not considered as secure and should be used as a minimum. All staff must connect to the network via the VPN when working away from the office.

Colleagues are responsible for ensuring the security of council property and all information, files, documents, data, etc. within their possession whilst working away from the office.

Staff must consider their surroundings whether working in an office or remotely. Unauthorised personnel or 'listening devices' such as Alexa or Siri could hear conversations. Similarly, unauthorised personnel could view information on screens or hard copy. Staff must assess their surroundings and prevent unauthorised disclosure of information (including the use of headsets in conference calls when others can overhear).

Users are not permitted to have the facility to print documents to a non-corporate printer when working remotely.

Further information on remote working can be found in the Bring Your Own Device Policy and Working Abroad Guidance on the intranet.

5.5 Data Protection and Security Impact Assessments

If a service area has a new project / process / service or there are changes to a project / process / service involving the use of personal data, a Data Protection Impact Assessment (DPIA) must be completed as a requirement under the legislation. A Supplier Security Assessment may also be required.

Colleagues must notify the council's Information Governance team immediately if they become aware of the implementation of a new system or the development of an existing system where Data Protection and Security Impact Assessments have not been completed.

Further information can be found within the Data Protection and Security Impact Assessment guidance on the intranet.

6. IT Security

6.1 Use of Equipment

All IT equipment provided to Colleagues to allow them to carry out their role is owned by Herefordshire Council. Colleagues must ensure that:

- Computer screens are locked to prevent unauthorised access when unattended. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action.
- They only install software that is available via the Company Portal or that has been approved via a request to the service desk.

- The configuration of any council owned portable computer device is not changed or altered.

- Asset registration numbers are not removed or defaced. In the event the asset sticker is loose or missing, colleagues should contact the IT Service Desk to request an asset sticker.

- Council assets are only used by council colleagues unless agreed by Information Governance and subject to a third-party agreement.

- IT equipment is not damaged as a result of neglect and ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, cost of repair and replacement may be recovered from the individual or service especially if a recurring event.

IT equipment can be used for personal use by staff so long as it is not used in relation to the operation of an external business and meets the security guidance in this policy. It must only be used by the authorised user e.g. not family members.

Access to the council's network will be withdrawn in an employee does not complete their information governance and information security mandatory training within timescale.

Users should follow the Working Abroad Guidance and seek approval from Information Governance **before** taking any council supplied IT equipment outside the United Kingdom. The equipment may not be covered by the council's normal insurance against loss or theft and equipment is at risk if confiscation by Airport Security personnel due to the encryption software installed on the device. If authorisation is not secured in advance and the equipment lost, stolen or confiscated the individual or service is liable to cover cost of replacement.

Herefordshire Council may at any time, and without notice, conduct a software or hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

Further information about colleagues' responsibilities when using IT equipment can be found in the Asset Management Policy on the intranet.

6.2 Internet Usage

The internet facility is made available for the business purposes of the council. The internet should be used to access anything in pursuance of a colleagues' work including:

- Access to and / or provision of information

- Research

- Training

- Electronic commerce (e.g. purchasing of equipment for the council)

Provided it does not interfere with their work, employees are permitted to use work devices for personal use of the internet in their own time (e.g. their lunch break). It is at the discretion of line managers to cease this provision.

The council is not responsible for any personal transactions an employee enters into using the corporate internet connection.

All access to the internet via a corporate device is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted.
- Producing access reports for line managers and auditors
- To maintain legal compliance
- To enable investigations where illegal / malpractice may have occurred.

Except where it is strictly and necessarily required for work, for example IT audit activity or other investigations, colleagues must not use their internet access to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- Individually subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe or, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programmes beyond the councils own systems.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter “money making” sites or enter or use “money making” programmes.
- Run a private business.

6.3 Email, calendar usage, conference facilities and Microsoft Teams

All emails that represent aspects of council business or council administrative arrangements are the property of the council and not of any individual Colleagues. Emails held on council equipment are part of the corporate record and provide a record of employee activities.

For avoidance of doubt, all email exchanges, conference facilities and Microsoft Teams using the council systems are owned by the council including personal exchanges and can be used for FOI, EIR requests and SAR’s, audits and investigations. The legal status of an email message is similar to any other form of written communication. Consequently, any email message sent is official communication from the council.

All emails that are used to conduct or support official Herefordshire Council business must be sent using a **“@herefordshire.gov.uk”** address or other recognised email accounts. Non-

corporate email accounts must not be used to conduct or support official Herefordshire Council business. Colleagues must ensure that any emails containing corporate information must be sent from an official email address.

Any emails containing personal and / or sensitive information must be sent securely.

Colleagues should be mindful of what they are sending by email and whether this is the best method of communication. Alternatives to email are available and guidance should be sought from Information Governance.

Emails sent between herefordshire.gov.uk addresses are held within the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communication network and are liable interception or loss and could be left within the public communications system.

In order to ensure that Herefordshire Council is protected adequately from misuse of electronic communications, the following controls will be exercised:

- Whilst respecting the privacy of authorised users, Herefordshire Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of electronic exchanges by authorised users to ensure adherence to this policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. During investigations an investigating officer has the right to access your emails without authorisation.

- Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the council's Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate.
- All users should be aware that electronic exchange usage is monitored and recorded centrally.

- Monitoring of content will only be undertaken by staff specifically authorised for that purpose.

- Access to another employee's email is strictly forbidden unless the employee or line manager has given their consent for specific work purposes whilst they are absent.

- Automatic forwarding of emails should be avoided. Council emails containing sensitive or personal information must never be forwarded to a personal email address.

Computer viruses are easily transmitted via email and internet downloads. If any user has concerns about possible virus transmission, they must report the concern to Hoople IT Service Desk.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.

- Must not download data or programmes of any nature from unknown sources.

- Must not attempt to alter anti-virus software installed on any computer which they use to access council facilities.
- Must not forward virus warnings other than to the Hoople IT Service Desk.
- Must report any suspected files to the Hoople IT Service Desk.
- Must comply with software updates.

In addition, the council will ensure that email is virus checked at the network boundary and at the host. If a computer virus is transmitted to another organisation, the council could be held liable if there has been negligence in allowing the virus to be transmitted.

Email must not be used for:

- The transmission of chain letters or other junk-mail of any kind.
- The transmission of materials that infringes the copyright of another person, including intellectual property rights.
- Activities that unreasonably waste staff effort or use of networked resources, or activities that unreasonably serve to deny the service to other users.
- Activities that corrupt or destroy other users' data.
- Activities that disrupt the work of 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 to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others or serves to harass or bully others.
- For 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.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material, which includes false claims of a deceptive nature.
- For so-called 'flaming' i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.

- For unfairly criticising individuals, stalking and shaming, including copy distribution to other individuals.

- For the creation or transmission of material which brings the council into disrepute.

The council has decided that the default setting for outlook calendars across the organisation will be 'open' for transparency and to support colleagues. This means that all users will be able to see limited details such as the time, subject and location of the meeting. The private function will only be utilised when essential for confidentiality. Further guidance around the recording of personal or sensitive information within calendar invites can be found on the intranet.

By default, the council does not record Teams meetings. Recordings can be made in specific circumstances if an adjustment is required and only at the consent of all parties. Consideration of storage recording conference calls is only used when absolutely necessary and only with the consent of all parties involved in the call.

Video conference and chat messages bring people together in a virtual workplace. Just like the office, the council's code of conduct continues to apply. The council will not tolerate offensive or derogatory behaviour.

Video conferencing and chat messages must not be used to download, process, store or transmit any unsuitable material that might be deemed illegal, obscene, offensive or derogatory.

Video conferencing should be treated the same as an in-person meeting, therefore your video should be on by default, with the only exception of low bandwidth causing a disruption to conducting business as a reason for not using video.

Colleagues should be mindful that the use of chat facilities is monitored, and that colleagues are expected to apply the same rules of behaviour as email usage. All chat messages are regularly deleted. Prior to deletion, information content is subject to FOI, EIR, SAR, audit or investigation.

Microsoft Teams is the corporate tool in place for staff and should be used when arranging or initiating video conferencing meetings. However, there will be times when a third party arranges a meeting via alternative tools such as Zoom or Webex. Council staff may participate in these calls providing the meeting can be accessed via a web browser or browser plugin.

6.4 Telephone Usage

The council provides 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 the council's business obligations:

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

Personal use of telephone services is permitted in emergency situations.

All users of mobile / smart telephones will sign to say that they understand their responsibilities when provided with a mobile phone. These responsibilities are detailed within the mobile phone procedure.

If your mobile phone is no longer required you must ensure that you return the device and all accessories e.g. phone charger, to ICT Procurement. Please refer to the Asset Management Policy for further information.

Any items not returned to IT will be subject to charge to the service – and the discretion of the service to forward that charge to the individual.

The council does allow access to certain systems via an authorised personal device – please refer to the Bring Your Own Device Policy for further information.

6.5 Use of Removable Media

Removable media devices include, but are not restricted to the following:

- CDs / DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering machines)

The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Only corporate owned removable media devices are allowed to connect to corporate equipment and systems, and store any information used to conduct official council business.

Requests for access to, and use of, removable media devices must be made to Hoople IT Services. Approval for their use must be given by your head of service.

6.6 Asset Management

Herefordshire Council must ensure the protection of all information assets within its custody. Each head of service or service manager is responsible for their team's information assets as the asset owner.

For the purpose of this policy, "important information assets" are identified as, but are not limited to, the following:

- Storage containing paper records.
- Computer databases and systems
- Data files and folders

Asset owners must ensure that:

- All information assets are assessed and classified according to their content. At minimum all information assets must be classified and labelled in accordance with section 6.1 of this document.
- An access control policy is in place for all information assets of which they are the owner.
- The council's Information Assets register is regularly updated.

6.7 System Access – Third Parties

Partner agencies or third-party suppliers cannot access the council's network without permission from Information Governance or Hoople IT Service Desk. Any changes to supplier's connections must be immediately sent to the IT Service Desk so that access can be updated or ceased.

Third party access agreements must be completed and authorised by Information Governance and the relevant director before access is given.

Guest Wi-Fi is available for third parties, which is bookable by an employee of the council.

7. Reporting Incidents

Some common examples of data security incidents are listed below. Please note that this list is not exhaustive and should be used as guidance:

- The loss of theft of information and equipment.
- Information sent to the wrong recipient.
- The transfer of sensitive or confidential information to those not entitled to receive it.
- Attempts to gain unauthorised access to data, information storage or a computer system.
- The unauthorised use of a system by an individual.
- The inappropriate disposal of sensitive or confidential information.
- The loss of computer media e.g. CDs, DVDs and Memory Sticks.
- Attempts to gain unauthorised access to secure areas.
- Management of information assets when a member of staff is suspended.
- Attempts to commit fraud.

All data security incidents should be reported to the Information Governance team as soon as they are detected.

All incidents will be investigated in order to establish facts and any corrective and / or preventive actions required. Not all incidents will need the same depth of investigation to find out the full

facts and determine what went wrong. If the investigation finds that a staff member did not follow council policy this may result in disciplinary action being taken.

8. Compliance

The council must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Anyone suspecting that there has been, or is likely to be a breach of information security, needs to inform their line manager and Information Governance immediately or follow the whistleblowing policy.

This policy and any associated procedures will be monitored by the Information Governance Steering Group. The Director, Governance & Law will be kept informed of any issues and instances of non-compliance regarding this policy.

9. Review

This policy will be reviewed as it is deemed appropriate, but at least every 3 years.

10. Approval and Document Control

Author: Claire Jacobs, Information Governance Manager
Status: Final
Responsible Corporate Director: Claire Porter, Director Governance & Law
Approval: Information Governance Steering Group (final draft) / SIRO (final)
Date Approved: 26 June 2025
Publisher: Herefordshire Council
Rights Copyright: Copyright of Herefordshire Council
Security classification: Open
Publication: Internal & External
Category: Corporate; information governance
Date for review: March 2028
Note: this is a merge of existing policies
Reference number: