Herefordshire Council

Information Security Policy 2021-2024

1. Introduction

Information is one of the council's most valuable assets and under principle 6 of the Data protection Act 2018 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. Herefordshire Council holds structured and unstructured information electronically both on premise and hosted in cloud IT Systems and physically in paper records which must all be suitably protected.

2. Purpose

This policy confirms the 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.

3. Scope

This policy applies to all staff, councillors, contractors, suppliers and partners. All employees 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.

4. Definition

This policy is the minimum standard which should be applied whenever employee's access council facilities and equipment; in addition, local procedures, standards and work accompany this policy. For the purposes of this policy 'employee' includes Full time and temporary staff, councillors, contractors, partners and suppliers.

5. Responsibilities and Commitment

The council's Management Board and Information Governance Steering Group are committed to ensuring that all aspects of information security are complied with to fulfil its statutory functions with this information security policy established so that:

- The requirements and activity outlined in this document form part of the mitigation to reduce risk to data security
- Highlights the key areas to effectively secure information

- It provides the framework for setting continual information security objectives

All employees 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.

6. Keeping Information Secure

6.1 Protective Marking

All written material must be considered as to whether it should be protectively marked, in accordance with the sensitivity of its content.

The protective marking used by Herefordshire Council is the following:
OFFICIAL SENSITIVE - Information that could have more 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.

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 OFFICIAL SENSITIVE.

Written information could be marked as confidential – which acts as a "warning" that information is only intended for the recipient(s).Legal privilege can be used in commercial negotiations and certain legal circumstances.

All information produced by the council is subject to FOI (freedom of information) and SAR (subject access requests) whether with or without protective markings.

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

6.2 Printing and Clear Desk / Clear Screen

The council has provided IT tools to ensure that documents do not need to be printed – this is to support information security, cost and environmental considerations. Documents must not be -printed unless it is absolutely necessary. If you do use printing facilities it is your responsibility to ensure that information is securely managed through storage or disposal.

Employees are required to operate a clear desk, in order to ensure that all information is held securely at all times. Documents left on desks or in meeting rooms at the end of a working day will be destroyed and the incident will be recorded as a data breach. Hard copy information is locked away when not in use, and only disposed of within the secure waste bins located within council properties when no longer required. This applies when working in the office, at home or in a shared space accessed by others.

All information must be stored appropriately if needing to be retained. 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, or whenever left unattended for long periods of time whether working in an office or at home.

In order to prevent inappropriate sharing of electronic information, employees must lock their computer screen when leaving their computer unattended.

Further information can be found in the printing and clear desk procedure on the intranet.

6.3 Passwords

Passwords are the first line of defence for 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.

Following guidance from the National Cyber Security Centre, Herefordshire Council has adopted the following password policy:

Passwords must be:

- At least 15 characters long
- Not based on anything which could be guessed easily by someone or obtained from personal information such as name, telephone number or date of birth
- Changed on indication or suspicion of compromise.

Hoople IT do periodically test the robustness of user passwords using password-cracking software. Staff will be required to change their password if it becomes compromised.

Herefordshire Council encourage the use of a pass phrase. This is a combination of words used as your password. Consider these 3 principles:

- Use 3 or more unrelated words, for example: “shop cod data day”
- Using special characters between words can increase security, for example: “shop&cod”data=day”

- The phrase should not be well know, like a saying from a film or book such as “Hasta la vista” or “to be or not to be”.

6.4 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 i.e. a café. Staff are however advised that public Wi-Fi connections are not considered as secure and should be used as a minimum. It is recommended that all staff must connect to the network via the VPN when working away from the office.
You are responsible for ensuring the security of council property and all information, files, documents, data etc. within your possession whilst working away from the office.

Staff must consider their surroundings, particularly when working remotely where unauthorised personnel, including ‘listening devices’ such as Alexa or Siri could otherwise hear audible conversations. Similarly, unauthorised personnel could view information on screens or hard copy paper. Staff must assess their surroundings and prevent unauthorised disclosure of information (including the use of headset 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 around working away from the office can be found on the remote working intranet pages.

6.5 Data Protection and Security Impact Assessments

Organisations that handle personal data need to monitor their ongoing operations, whether they are dealing with clients, employees, or the public in general.

Completion of a Data Protection Impact Assessment (DPIA) is a requirement of Article 35 of the General Data Protection Regulation. Appropriate Data Protection and Security Impact Assessments must be completed when a new system or service is introduced or when there is a change to existing systems and services. These include:

- The completion of a Data Protection Impact Assessment
- The completion of a Supplier Security Questionnaire to include an assessment regardless of whether internal or external /cloud hosted IT systems.

Commissioners, Providers and Partners 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.

7. IT Security

7.1 Use of Equipment

All IT equipment provided to staff to allow them to carry out their role is owned by Herefordshire Council. Employees 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.
- Staff shall only install software that is available via the Software Centre 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, contact the IT Service Desk to request an asset sticker.
- Council assets are only used by council employees unless agreed by Information Governance and subject to a third party agreement.
- That IT equipment is not damaged as a result of neglect and ensure 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. Also, only by the authorised user e.g. not family members.

If staff do not complete their information governance and data management mandatory training within timescale, access to the council's network will be withdrawn.

Users should seek approval from information governance and their head of service 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 the equipment is at risk of 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 employee's responsibilities when using IT equipment can be found in the asset management policy on the intranet.

7.2 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 your work including:

- Access to and/or provision of information
- Research
- Training
- Electronic commerce (e.g. purchasing equipment for the council).

Provided it does not interfere with your work, employees are permitted to use work devices for personal use of the Internet in your own time (for example during your lunch-break). It is at the discretion of your line manager to cease this provision.

The council is not responsible for any personal transactions you enter using the corporate internet.

The provision of Internet access is owned by the council and all access 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 your work, for example IT audit activity or other investigation, you must not use your 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 to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs beyond the council 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" programs.
- Run a private business.

7.3 Email, calendar usage, conference facilities and Instant Messages

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. Employees must ensure that any emails containing corporate information must be sent from an official council email address. Any emails containing personal and/or sensitive information must be sent securely. Employee's 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.

All emails that represent aspects of council business or council administrative arrangements are the property of the council and not of any individual employee. 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 instant messages using the council systems are owned by the council including personal exchanges and can be used for FOI, SAR, audits and investigations. The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent is official communication from the council.

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.
- 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 exchanges 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. During investigations an investigating officer has the right to access your emails without authorisation.
- Emails sent between herefordshire.gov.uk address 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 communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system.
- Automatic forwarding of emails needs due consideration and only done for a valid reason respecting the intention of the originator (both internal and external) and where relevant requests made to them to forward the information. 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. Full use must therefore be made of the council's anti-virus software. 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 programs 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.

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, to other organisations
- 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
- 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, that 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 have 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. To utilise the private function only when essential for confidentiality. Further guidance around the recording of personal and or sensitive information within calendar invites can be found on the intranet.

Video conference access and licences are available to employees via IT or member support (for councillors). Any hacked conference calling within the council's licence must be reported to IT immediately. Third party users are responsible for the security of their own licences.

By Default the council must not record conference calls unless an adjustment is required and only at the consent of all parties. Consideration of storage recording of conference calls is only used when absolutely necessary and only with the consent of all parties involved in the call.

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

Video conference and Instant Messaging 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.

Employees should be mindful that the use of instant messaging and conference chat facilities is monitored, and that employees are expected to apply the same rules of behaviour as email usage. All instant message and conference chats are regularly deleted. Prior to deletion, information, content is subject to FOI, 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. The only time when a camera is not used is when bandwidth does not allow.

7.4 Telephone Usage

The council provide 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.

If you require a mobile/smart phone to carry out your role you must discuss your requirements with your line manager and follow the mobile phone request procedure.

To minimise costs our standard contracts do not budget for heavy or frequent internet usage. If your work requires frequent use of the internet from your phone or functions such as tethering you must consult your manager and ICT Procurement who will advise on the best options (which could include cost to the service).

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 that are 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 do provide the capability to allow personal devices to access a corporate mailbox (email, calendar, contacts and tasks) as an alternative to providing a smart phone (not as well). Approvals must be supported by your line manager.

Due to associated risks, the BYOD (bring your own device) policy must be read and staff must sign to the terms and conditions of this service. Requests can be initiated via the Service Desk.

7.5 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.

Should access to, and use of, removable media devices be approved employees must follow the removable media procedure at all times. This is available on the intranet.

7.6 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 1 of this document
- An access control policy is in place for all information assets of which they are the owner.
- The Councils Information Asset register is regularly updated.

7.7 System Access – Third Parties

Partner agencies or third party suppliers must not be given details of how to 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. All permissions and access methods must be controlled by Information Governance via third party agreements.

Partners or third party suppliers must contact the Hoople IT Service Desk before connecting to the Herefordshire Council network and a log of activity must be maintained. Remote access must be disabled when not in use.

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

8. 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 or 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 by emailing informationgovernance@herefordshire.gov.uk.

All incidents will be investigated in order to establish facts and any corrective and/or preventative 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.

9. Compliance

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

The council must take technical and organisational measures to protect personal 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 personal data understands that they are contractually responsible for following good data protection practice
- Everyone managing and handling personal data is appropriately trained to do so
- Everyone managing and handling personal data is appropriately supervised.

If any user is found to have breached 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.

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.

10. Review

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

11. Approval and Document Control

Author: Helen Worth, Information Governance Manager
Status: Final
Responsible Assistant Director: Natalia Silver, Assistant Director Corporate Support
Approval: Information Governance Steering Group (final draft) / SIRO (final)
Date Approved: 09.09.2021 (final)
Publisher: Herefordshire Council

Security classification: Open
Publication: Internal
Category: Corporate; information governance
Date for review: September 2024
Note: this is a merge of existing policies
Reference number: