Herefordshire Council

Reference number	
Approved by	**Information Governance Steering Group**
Date approved	**15/01/2016**
Version	**1.3**
Last revised	**June 2018**
Review date	**June 2021**
Category	**Information Assurance**
Owner	**Information Governance**
Target audience	**All staff**

INFORMATION SECURITY PERSONAL RESPONSIBILITES

Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

DOCUMENT HISTORY

Document Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
0.1	Draft				
0.2	Draft		Change of Name	All	
0.3	Draft		Merge of other guidance document to form one policy.		
0.4	Draft		Changes made to reflect comments received during consultation		
1.0	Final	18/01/2016			January 2019
1.1	Issued	17/05/2016	Updated to reflect Steering Group Comments and SWAP Audit findings		January 2019
1.2	Issued	07/06/2018	Updated to include asset management		January 2019
1.3			Updated to reflect GDPR and tethering changes		June 2021

Contents

Purpose

The purpose of this document is to inform all staff, councillors, contractors and partners of their responsibilities for handling and protecting the information they work with.

Scope

Within Herefordshire Council we amass a great deal of confidential information about our employees, customers, third parties, research, and financial status. Most of this information is now collected, processed and stored electronically on computers and transmitted across the network to other computers. Should confidential information fall into the wrong hands there could be significant repercussions.

Every person handling information or using Council information systems is expected to comply with the Council's policies and procedures. The purpose of this document is to highlight your key responsibilities and actions that you should take when handling data.

1.0 Protectively Marking Information

All documents must be considered as to whether they should be protectively marked, in accordance with the sensitivity of their content.

The protective markings used by Herefordshire Council are:

Classification	Description
UNCLASSIFIED	These are documents generated and used daily for routine communication and require no special handling requirements. This includes information made available to the public.
OFFICIAL	The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.
OFFICIAL – SENSITIVE	OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. In such cases where there is a clear and justifiable requirement to reinforce the ''need to know''. 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 under exceptional circumstances.

The originator must:

- Place a protective marking on every page of an electronic document in either the header or the footer.
- The protective marking of an email must be placed in the subject line.
- Consider to what level the document must be protected based on:
    - The degree of risk to Herefordshire Council should the data be disclosed
    - The content of the data
    - The intended audience of the data
- Regularly review the protective marking of the documents they have created.
- Communicate OFFICIAL – SENSTIVE information/documents securely. i.e. by secure email
- Store OFFICIAL – SENSITIVE information/documents securely.
- Destroy OFFICIAL-SENSITIVE information/documents securely. i.e. using a cross shredder

Further information about how to apply a protective marking can be found within the Handling Information Procedure.

2.0 Storing Paper Information

All information must be stored appropriately. Paper records containing sensitive information must be locked away in appropriate storage when not in use, or whenever left unattended for long periods of time.

It is the responsibility of the individual to make sure that information, records or data is not left on desks overnight where it can be seen or handled by unauthorised persons.

3.0 Clear Desk and Printing

Herefordshire Council has a clear desk policy in place in order to ensure that all information is held securely at all times. Work should not be left on desks unattended and should be removed from view when unsupervised.

- Paper copies of documents should be scanned onto the network and stored in a drive.

- Nothing should be left lying on printers, photocopiers or fax machines at the end of the day.

- All items sensitive to the council, our customers or containing personally identifiable information will be stored securely when the area is unattended, (e.g. lockable safe or)

- No sensitive council or customer information or 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 sensitive council and customer documents or documents with personally identifiable information must be placed in confidential waste bins when no longer needed and ready for disposal.

Remember, when you are not working at your workstation there could be a business requirement for other staff to use that station.

It is corporate policy that documents are not printed unless it is absolutely necessary. If you do use printing facilities the following must be observed:

- If using a shared printer without secure print, documents must be collected immediately and not left for casual viewing or inspection.
- 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 document using council equipment in general is not permitted. If required authorisation must be obtained from your line manager.

4.0 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.

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least eight characters.
- Contain a mix of alpha and numeric, with at least one digit
- Free from identical or consecutive characters or numbers.
- 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.

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Herefordshire Council systems.
- Do not use the same password for systems inside and outside of work.

5.0 Use of IT Equipment

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Computer screens must be locked to prevent unauthorised access when unattended and screens will lock automatically after a 5 minute period of inactivity, in order to protect information. A screen saver with password protection enabled will be used on all PCs. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action.
- Users will not install or update any software on to a Council owned portable computer device.
- The installation of software on all corporately owned devices, including computers and mobile devices, requires authorisation. Requests for software installations must be raised with the Service Desk.
- Users will not change the configuration of any Council owned portable computer device.
- Users will not install any hardware to or inside any Council owned portable computer device, unless authorised by Herefordshire Council. (e.g personal mobile phones should not be connected to a corporate device to charge them)
- Users will allow the installation and maintenance of Herefordshire Council installed Anti-Virus updates immediately.
- Users must not remove or deface any asset registration number.
- All requests to access applications must be authorised by line managers.
- User requests for upgrades of hardware or software must be approved through the change control procedure.
- The 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. Only software supplied and approved by Herefordshire Council can be used (e.g. Word, Excel, Adobe, etc.).
- No family members may use the IT equipment.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, Herefordshire Council may recover the costs of repair.
- The user should seek advice from Herefordshire Council 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 liable to be confiscated by Airport Security personnel.

- Herefordshire Council may at any time, and without notice, request software and 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.

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

- Use of computer resources for the purposes of fraud, theft or dishonesty.
- 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 council procurement procedures, or
    - for which the council does not hold a valid program licence, or
    - Which has not been the subject of formal virus checking procedures.
- Storing/processing/printing of data for a purpose which is not work related.

6.0 Internet Usage

The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this guidance.

Your Council Internet account should be used to access anything in pursuance of your work including:

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

At the discretion of your Line Manager and provided it does not interfere with your work, the Council permits personal use of the Internet in your own time (for example during your lunch-break).

The Council is not; however, 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 by lack of capacity.
- The filtering system monitors and records all access for reports that are produced for line managers and auditors.

Access to the following categories of websites is currently blocked using a URL filtering system:

- Illegal.
- Pornographic.
- Violence.
- Hate and discrimination.

- Offensive.
- Weapons.
- Hacking.
- Gambling.
- Dating.
- Radio stations.
- Games.
- Streaming Media e.g. You Tube where it is not a Herefordshire Council initiative

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.
- 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.
- Download any software that does not comply with the Council's Software Policy

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 Council policies.

7.0 Email Usage

All emails that are used to conduct or support official Herefordshire Council business must be sent using a "@Herefordshire.gov.uk" or "@Herefordshire.gcsx.gov.uk" address.

Non-work email accounts **must not** be used to conduct or support official Herefordshire Council business. Councillors and users must ensure that any emails containing corporate information must be sent from an official council email. Any emails containing personal and/or sensitive information must be sent from a GCSx email.

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 considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Herefordshire Council business should be considered to be an official communication from the

council. In order to ensure that Herefordshire Council is protected adequately from misuse of e-mail, the following controls will be exercised:

- All official external e-mail must carry the following disclaimer:

'Any opinion expressed in this e-mail or any attached files are those of the individual and not necessarily those of Herefordshire Council. This e-mail and any attached files are confidential and intended solely for the use of the addressee. This communication may contain material protected by law from being passed on. If you are not the intended recipient and have received this e-mail in error, you are advised that any use, dissemination, forwarding, printing or copying of this e-mail is strictly prohibited. If you have received this e-mail in error please contact the sender immediately and destroy all copies of it."

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 email 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 email 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 with 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.

All emails containing personal or sensitive information must be sent securely. Refer to the Email procedure for further information.

Automatic forwarding of emails must not be set up without prior authorisation from Head of Service. Council emails containing sensitive or personal information must never be forward to a personal email address.

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Herefordshire 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 ensure that an effective anti-virus system is operating 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:

- For the transmission of chain letters or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of OFFICIAL or OFFICIAL-SENSITIVE material concerning the activities of the council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For 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.
- For 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, including copy distribution to other individuals.
- For publishing to others the content of messages written on a one-to-one basis, without the prior express consent of the author. i.e. forwarding of email chains.
- For the creation or transmission of material which brings the council into disrepute.

8.0 Telephone Usage

The council 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 the council'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.

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 Procurement who will advise on the best options.

All users of mobile/smart telephones will sign to say that they understand their responsibilities when provided with a mobile phone.

- Your Council mobile or smartphone must require a PIN or password to unlock.
- Mobile telephones must not be left unattended in vehicles
- You must not store sensitive Council or customer information or sensitive personally identifiable information on mobile phones or smartphones.
- The tethering of smartphones to other equipment to provide internet access is by exception only for access issues. A business Case will need to be approved by your line manager in order to tether to your mobile phone.
- You must not use the internet access via your phone for bandwidth intense applications such as watching television or films.
- You may not install applications or games onto your smartphone including ring tones
- You must not remove the SIM card from your phone and place it into another handset
- You must not use your phone for taking and storing personal photographs
- You must not take your phone out of the country unless authorised by IG and Head of Service or AD.
- 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 operate within the law when using a mobile phone while driving any vehicle (driving means whenever the engine is switched on, even if the vehicle is stationary).

If your phone is faulty you need to call EE Customer Services on 158 direct from another EE mobile phone, or 07973 100158 from any other phone.

If your phone is lost or stolen you need to:

- Advise the service desk.
- 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.
- Contact EE Customer Services (07973 100158), their representative will require the police reference number from you and a full description of the event leading to the loss/theft before replacing the phone. Get a timescale for the replacement.
- Advise your manager.

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 will be replaced by IT services and charged to the relevant cost code.

9.0 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.

Non-council owned removable media devices **must not** be used to store any information used to conduct official Council business, and **must not** be used with any Council owned or leased IT equipment.

Requests for access to, and use of, removable media devices must be made to Hoople IT Procurement. Approval for their use must be given by your Head of Service.

Should access to, and use of, removable media devices be approved the following must be adhered to at all times.

- All removable media devices and any associated equipment and software must only be purchased and installed by Hoople IT Services.
- The only equipment and media that should be used to connect to Council equipment or the Council network is equipment and media that has been purchased by the Council and approved by the Head of Service or has been sanctioned for use by the Head of Service.
- Therefore removable media should not be the only place where data obtained for Council purposes is held.
- Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

- In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.
- Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.
- All data stored on removable media devices must, where possible, be encrypted.
- It is the duty of all users to immediately report any actual or suspected breaches in information security to Information Governance who will appoint an investigating office to investigate the incident
- Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to Information Governance
- Damaged or faulty removable media devices must not be used. It is the duty of all users to contact Hoople IT Service Desk should removable media be damaged.
- Virus and malware checking software approved by the Hoople It Service Desk must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by virus checking software products, before the media is loaded on to the receiving machine.

- Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity.
- Removable media devices that are no longer required, or have become damaged, must be returned to Hoople ICT for destruction.

Further information can be found within the Removable Media Procedure.

10.0 Working Remotely

This section of the guidance applies to your use of the Council network whenever you are working away from council premises for example at home.

You are responsible for ensuring the security of Council property and all information, files, documents, data etc. within your possession.

Additional care must be taken when working with information or systems outside of the secure Council offices.

When working remotely you must:

- not leave equipment and files unattended in public areas;
- 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 discuss or show sensitive Council 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 Council business, locking equipment and sensitive information away or storing out of sight;
- take due care and attention of portable computer devices when moving between home and/or another business site:

- Portable devices must be kept out of sight in a locked boot and then only retained there for short intervals.
- Portable devices must not be left in cars overnight or for long periods of time.
- keep your passwords secret;
- inform the Police, Information Governance and Service Desk as soon as possible if records, equipment or any computer equipment on which you do Council work has been stolen (you will need a police crime number and report);
- ensure that any work which you do remotely is saved on the Council's system or is transferred to Council 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;

Users are not permitted to have the facility to print documents to a non-corporate printer when working remotely unless this has been authorised by Information Governance.

Council equipment may not be used by others i.e. family and friends etc.

If you intend to use your own IT equipment to connect from home it will only provide specific application access or connect through a terminal style connection. 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 Council information or systems.

11.0 Sharing Information

Fundamentally, sharing information involves:

- Balancing our interests and that of the organisation with which we are sharing with the rights and freedoms or legitimate interests of the data subject.
- always seeking consent first where appropriate
- asking the requester to provide the gateway and what specific information is actually needed by them
- asking if everything being shared is relevant and proportionate to the request

There as 7 key questions to ask yourself when considering whether information should be shared.

Is there a clear and legitimate purpose for sharing information?
All sharing must comply with the law relating to confidentiality, data protection and human rights. Establishing a legitimate purpose for sharing Information is an important part of meeting these requirements. Other legislation may also have a bearing for example:

Children Act 1989
Mental Capacity Act 2005
The Police Act 1996

Does the information enable a living individual to be identified?
If the information is anonymised to an acceptable level it can be shared. If the information is about an identifiable individual or could enable a living person to be identified when considered with other information, then it is subject to the Data Protection Act and other laws. Consent must be sought from the individual unless it would be unsafe to do so.

Is the information confidential?
Confidential information is:

Personal information of a private nature
Information not already lawfully in the public domain or available from another public source
Information shared in circumstances where the person sharing could reasonably expect it not to be shared with others.

Is there consent to share?
The consent given should be informed which means the person giving consent understands why information needs to be shared, what information will be shared, the purpose for sharing the information and any implications. Written consent is preferable and it should be sought at the before sharing if possible. Individuals can withdraw consent at any time.

Is there sufficient public interest to share?
Even when consent is refused it may be in the public interest to share information. Examples of public interest would be preventing significant harm to children, preventing serious harm to adults, preventing crime and disorder. Carrying out a risk assessment will help establish the need for sharing.

Is information being shared securely and appropriately?
The sharing of information should be done in a proper and timely manner and in accordance with both the Data Protection Act 2018 and any organisational policies and procedures. For example using secure email, recorded delivery.

7. Has the information sharing decision been properly recorded?
Any decision to share or not to share confidential information should be recorded. Where the decision is to share, the information shared and who has received it should be recorded in case of a later challenge.

12.0 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.
- 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 equipment.
- 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 emailing by 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.

13.0 Third Party Access to the Council Network

Partner agencies or 3rd 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.

Partners or 3rd 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.

14.0 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.

The process of identifying important information assets should be sensible and pragmatic.

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

- Filing cabinets and stores containing paper records.
- Computer databases.
- 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 updated is regularly updated.

Compliance

Failure to follow the procedures described in this document may impact on good employee relations and the reputation of Herefordshire Council. 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 Council 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.

Relevant Guidance and Procedures

Guidance and procedures are available on the intranet to support staff in keeping information safe.

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years Policy review will be undertaken by the Information Governance Steering Group