CABINET

DATE OF MEETING: **3 DECEMBER 2020**

TITLE OF REPORT: **IT SECURITY POLICY**

Report of: **Head of Corporate Services**

Cabinet Member: **Councillor James Radley, Deputy Leader and Finance**

1 PURPOSE OF REPORT

1.1 To present the revised IT Security Policy for subsequent approval by Cabinet.

2 RECOMMENDATION to Council

2.1 That Cabinet approve the IT Security Policy at Appendix A.

3 BACKGROUND

3.1 It is best practice that the IT security policy is reviewed and revised annually to ensure that our staff are guided and comply with the most up to date guidance and security controls. Compliance is mandatory and is required to safeguard both individual users and the Organisation as a whole.

4 NEXT STEPS

4.1 Hart users will be supported through the application of this policy with training workshops where questions can be raised or confirmation and clarification provided.

Contact Details: **Alistair Trigg, email: alistair.trigg@hart.gov.uk**

APPENDICES:
Appendix 1 – IT Security Policy

ICT Security Policy

Owner: Alistair Trigg

Date: November 2020

Expiry date: November 2021

Distribution: All HDC staff and members

Version: 2.

Document History

Issue	Date	Purpose	Author
1.7	01/04/2016	Annual update to ensure compliance with Govt Connect	Alistair Trigg
1.8	01/02/2019	Annual update	Alistair Trigg
1.9	19/10/2020	Refresh policy draft incl. merge of Acceptable Use Policy	Steve Bennett
2.0	20/11/2020	Review, take our duplication and add key points section at back	Emma Foy

Review and approval process for current version

Reviewer	Date	Review/ approve
IT & Information Governance	19 October 2020	Review
Staff consultation via Change Group	3 November '20	Review
Management Team	10 November 2020	Approve
Overview & Scrutiny	17 November 2020	Review
Cabinet	3 December 2020	

Contents

1. Introduction

This purpose of this policy is to ensure that all users of Hart District Council ICT systems and resources including hardware, software and telephony are given guidance on best practice for the secure and efficient use of the Council's systems.

2. Scope

This policy applies to the use of Hart District Council (the Council) IT systems assets and information whether working within the local offices or working remotely on Council business. This policy applies to all Council users including staff, Councillors, contractors, or temporary staff and applicable third parties.

The policy is designed to:

- Promote a level of awareness for the need for ICT security to be an integral part of the day to day operation so that all users understand the need for security and their obligations on how they use our systems
- Provide secure information systems, computer installations and networks that are available to users when required
- Safeguard information from unauthorised disclosure or modification and that data remains confidential, accurate and complete

This policy applies to all information held in manual and electronic form.

3. Related Policies and Procedures

All related policies and procedures are available on the Council's intranet including:

- Information Security Incident Management policy
- Remote Access Policy

4. Security, Support & Fault Reporting

If you suspect that a breach of security has occurred (loss of sensitive/personal data, theft /lost equipment, PC infected with a virus/malware, another person has guessed your password or gain unauthorised access, etc), or inappropriate content detected please contact IT Support immediately. If you suspect there has been a data breach, this should be reported to the Information Governance Officer within 72 hours as required by the General Data Protection Regulation You should also refer to the Information Security Incident Management policy.

IT assistance and support is available to you across all sites. All hardware and software faults and security incidents must be logged with IT Support.

Users can contact IT support by emailing Capita IT support:

- servicedeskruddington@capita.co.uk
  0808 1643093

The internal IT support team should be copied in to make them aware:

- Office365@hart.gov.uk
  01252 774252

5. Computer Viruses & Malware

Computer viruses represent a significant threat to the Council. It is your responsibility to ensure that they do not knowingly infect any of the Council's computer systems or network. Viruses can be propagated in a number of ways including links and attachments in e-mails or from a compromised internet webpage accessed from the network and via external storage media e.g. CD and USB memory sticks.

All Council laptops and PCs have the Council's corporate virus checking software installed on them - this must not be deactivated. If your antivirus checking software detects a virus, stop using your PC and contact IT Support immediately.

All storage media coming into the Council premises must be scanned for viruses, even those originating from an individual's department that is being returned. Contact IT support if you would like any advice on using the anti-virus scanning software.

6. Email Usage

The Council provides access to e-mail to help staff perform their day to day functions. Any inappropriate use of the e-mail system reflects directly on the Council and may damage the Council's reputation.

You must not have any expectation of privacy when using e-mails, to or from anyone inside or outside the Council. If the contents of the email or attachments are confidential you should consider how to protect them or contact IT Support for help Use of personal e-mail accounts such as Hotmail is prohibited for use on Council business correspondence.

E-mails are legally binding communications and can be used as evidence in disciplinary and legal proceedings. Once the e-mail has been sent, you cannot control its onward distribution to other persons. Similarly, you cannot control where the e-mail is stored. Before sending, you should consider any impact on the Council and if the content may commit the Council to any particular course of action, does it contain personal opinions, is material that may offend others, or contains information that the you would not want to forward to others.

Spam is the common term used to refer to unsolicited or junk e-mail, or e-mail from an unknown source that you did not request. Please note that this explicitly excludes e-mails to which you have subscribed. Many spam e-mails may appear to be inoffensive based upon its title, but the content might often be offensive. Increasingly, spam or junk e-mails may also contain malware, viruses, or scams to obtain your personal data and is commonly known as phishing.

To avoid being added to spam or junk mailing lists:

- Your Council email address should not be used for non-business-related purposes
- You should never respond to spam email if this confirms the Council email address.

To avoid being target of a successful phishing attack, you must:

- Not open any files attached to an email from an unknown, suspicious or untrustworthy source
- Not open any files attached to an email or follow any embedded links, unless you know what it is and is from a reliable known source. Many viruses can replicate themselves and spread via email
- Not open any files attached to an email if the subject line is questionable or unexpected. If there is a business need to do so, only save files from a trusted source to your hard drive first and manually scan it before opening
- Change your password immediately if you have clicked on any links within a suspicious email
- You must take care when replying or forwarding to ensure that only relevant parties are included
- Delete chain emails and place junk email in the Junk email folder. Do not forward or reply to any to them unless this is to report them to office365@hart.co.uk
- Do not download or accept any files from unknown individuals or organisations. If in doubt, contact IT support for advice
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. If possible, verify that the anti-virus program checks the files on the download site. If any doubt, you should not download the file at all and obtain advice from IT support
- Check that your anti-virus software is up to date
- Not open, download, or execute any files or email attachments that are suspicious
- Not provide your email or login id and password into any links, or online web page requesting this information. Be aware of fraudulent emails requesting this information.

You must ensure that the laptop can install updates for the virus checking software and receive the latest updates to programs and operating system.

If you suspect or know of a virus on your system do NOT ignore it. Disconnect your machine from the network and report it immediately to IT Support providing details such as time and possible cause of infection and any error messages.

7. Internet Use

The Council provides you with internet access and electronic communications services as required for the performance and fulfilment of job function and responsibilities. These services are for Council business purposes only. They must NOT be used for non-Council business activities. Occasional and reasonable personal use of the Councils internet services is permitted provided this does not interfere with day to day performance.

You should have no expectation of privacy while using Council owned IT equipment and resources. Information passing through or stored on company equipment is audited and will be monitored.

All access to the internet is logged and can be used for audit purposes. Access to several non-business-related sites is blocked. If you download information from the Internet, you must comply with applicable copyright laws. It is also your responsibility to verify the

accuracy and authenticity of downloaded information, including a scan for possible virus infection.

8. System access

Requests to provide access must be made through the relevant Line Manager or Head of Service. Network passwords will be set to prevent unauthorised access to data. The use of unique passwords is especially important in the case of laptop/notebook PCs which are highly portable and less physically secure. Users must not disclose their password to anyone.

In some exceptional cases that have been authorised by the IT Client Manager a shared PC may have a network password known by several users within an office to enable access. Where this is unavoidable, secure mechanisms, such as a restricted and locked office, should exist to ensure access to the PC is solely used by authorised personnel.

Unique usernames will be allocated by the system administrators. Wherever possible, these will be consistent across applications. Access levels will be determined and implemented by systems administrators for each application area. Likewise access to any shared resource on the network e.g. printers, can be given by the network administrators.

Passwords should be used to protect all systems and should not be written down or disclosed to others not properly authorised to use them. You will be held liable for any misuse of a computer resulting from use of their password/username. See Appendix A for Password Policy

9. Software

Only software installed or authorized for installation by the Council may be used solely for the purpose for which it was installed. This applies to all software including screen savers.

You must not:

- Copy software for use on another machine
- Install any software on PC's or laptops without prior authorisation from the Council's Joint Chief Executive or IT Client Manager
- Tamper with the standard hardware/software configurations on PC's or laptops,
- Disable or deactivate any element of the standard PC or laptop configuration, including disk encryption, screen saver password and anti-virus software.

10. Patching

All system patches must undergo appropriate testing prior to deployment into the live or production environment. Where a vulnerability has been identified and the Council has been notified of the associated risks including where adequate testing of patches is not possible, the Council must evaluate the risks for any delay in patching those system.

Following successful testing, a patch should be scheduled for deployment and follow standard change management processes. At this stage a final assessment should be performed to ensure that the patch classification stands. It may also be appropriate to schedule deployment to co-inside with additional deployments.

The deployment of all patches must be managed via a standard change control process that includes documented back-out process.

You must shut down all systems that they access and reboot the laptop or PC at least once a week to ensure that temporary files are cleared, and any system patches and updates can be applied.

11. Change Management

Changes to the Council's operational systems must be controlled with a formally documented change control procedure. The change control procedure should include references:

- Ensuring changes are submitted by authorised personnel only
- A description of the change and business reasons
- Information concerning the testing phase
- Impact assessment including business, security and operational risks
- Formal signoff and approval process
- Maintaining appropriate version control where necessary
- Communication to all relevant parties of the changes
- Procedures for aborting and rolling back the change if problems occur
- Process for tracking and audit
- Ensure all user and operational documentation are updated.

12. Development and Test Environments

When introducing new systems or making major changes to existing systems, processes should follow best practice for their documentation, specification, testing, quality control and managed implementation. Any such development and testing of new systems and software must be conducted within in a segregated environment from the live or production systems and software environments.

13. Screen Savers

All desktops and laptops are configured with the Council's screen saver software enabled. This will lock the screen after 15 mins inactivity and require you to input your password. Applications may also log you out after a period of inactivity. Press Ctrl-Alt-Delete and press <Enter> or Windows key and L to activate the screen saver before leaving the device for any period of time.

14. Storage of Business Data on SharePoint and OneDrive

All data must be stored in corporate systems or on O365 SharePoint or the OneDrive that you have access to. Do not store Council business data, particularly personal data relating to customers on any personal device or any external cloud hosted storage systems or device. You must not install any additional software applications on your PC without prior approval.

You should avoid saving documents locally on a desktop computer or laptop, as they are not backed up and information may be irretrievable if the device fails or is stolen. This includes synchronising SharePoint and OneDrive to a local device without IT authorisation.

You must not circumvent SharePoint security measures. Corporate data/information must only be stored on team sites. You must not attempt to access content for which you do not have permission.

All staff must maintain the supported infrastructure setup by filing the documents via Adding Properties and not creating folders within folders. Site owners are responsible for managing the use of SharePoint in their area and are accountable for their actions.

Site owners are responsible for the custody or operation of their SharePoint sites and are responsible for proper authorisation of user access. Data used in SharePoint must be kept confidential and secure by the user.

You must ensure that permissions to document libraries are appropriately set and maintained to ensure the security of information. You must ensure that private or personal documents are secured (through the use of the 'only me' function) to ensure the security of information.

Data can be shared with external people/organisations using the 'External sharing' SharePoint site. All documents shared must be removed once the need to share has expired. Any sensitive data shared in this way must be done with the appropriate set up of SharePoint permissions to ensure the security of that data.

Only personal documents should be saved to OneDrive. OneDrive must not be used as a replacement for corporate shared document management. OneDrive documents could include training or meeting notes, certificates, 121 meeting notes and should not be kept for longer than necessary.

15. Confidential Media

All paper records and removable media (e.g. USB memory, CDs) containing confidential and personal information must be stored securely and must be encrypted. They must not be left on a desk. Please observe the Council's clear desk policy.

Confidential records must be kept for the required period as defined under the Council's data retention schedule. Records must be destroyed securely when no longer required.

16. Laptops and phones

You are responsible for the security of mobile devices allocated to you including laptop, mobile phone, tablet, etc.

- Do not leave mobile equipment unattended in a public area
- Do not leave IT assets in the boot of a vehicle for any longer than is necessary

When accessing confidential or personal data, be aware of your surroundings. Take reasonable precautions to safeguard passwords, data, and mobile devices. Mobile devices must be protected with a minimum 6-digit pin. Ensure your mobile device is placed in a

locked state when not in use. You must not connect any non-authorised device to the network or IT systems as there is no guarantee of security or confidentiality with the use of free wi-fi connection. Using the phone for personal calls should not interfere with daily business and wherever possible be made outside of working hours.

Employees are expected to use the internet responsibly and productively. Excessive personal internet browsing, including social media use, is not permitted.

Calls to premium rate numbers and overseas are not permitted, unless there is a real business need and authorisation has been provided by the relevant Head of Service.

When driving, staff are expected to comply with the Road Vehicles (Construction and Use) (Amendment)(No4) Regulations 2003, which prohibit the use of handheld mobile devices at all times when driving

All portable equipment such as laptops, PDA's/tablets, mobile telephones, including USB disks, DVDs, CDs must not be left unattended when taken out of Council buildings.

Inform the police and IT Support immediately of any item stolen or lost that you conduct Council business with.

17. Security Incidents

If you suspect that a breach of security has occurred (loss of sensitive or personal data, theft /lost equipment, PC infected with a virus/malware, another person has guessed your password or gain unauthorised access, etc), inappropriate content detected please contact the IT Support immediately.

18. Business Continuity

The Council has a business continuity plan that defines how it will recover in the event of a disaster. You must ensure that you are aware of your department's business continuity responsibilities and know what you are expected to do in the event of a disaster.

19. Physical access

The Council's priority is to ensure that there is always adequate security at the office which reduces the physical risks from unauthorized access, damage and interference with its offices and the information they contain.

Further secure areas such as computer rooms require a higher level of authorisation and are guarded by a code entry access point. For all other levels of security, the Council provides lockable cabinets and desks for highly confidential documents, tapes, DVDs, and CDs as required by
particular areas of the business.

Every Hart employee is issued with an electronic entry pass card by the Facilities Management team subject to a formal request from the Head of Service. No person should gain entry to the Council's offices using a cardkey other than the person for which it was issued.

Visitors are issued with a temporary pass and must be accompanied to and from meeting rooms. Only visitors to the ground floor public areas (including the meeting rooms) are exempt from being issued with a pass. All contractors must be supervised by a representative from the department that engaged them.

All employees, Members, temporary staff, and contractors must always wear or carry their identity card with them at all times. Any unidentified person not wearing an identity card or pass should be approached for identification and asked who they are visiting. A visitor or contractor who is lost will accept your help. Professional intruders are experts at being believable, hence the need for challenge. Anything suspicious should be reported to reception or a senior manager immediately.

Electronic equipment is located within the offices for monitoring of risks from theft, fire and smoke. The Council conforms to the Health Act 2006 which states that its premises must be smoke free if they are used as a place of work. This also includes any vehicles used for Council business. Eating and drinking is not permitted in the computer server room. All portable computer equipment must be signed out from the department.

Information systems are provided strictly for business purposes. This includes all devices, servers, workstations, laptops. mobile phones and tablets. Software must be used strictly in accordance with the licensing agreement.

20. Personal and confidential data management

You may have access to personal and confidential data relating to the Council and its customers. You should exercise due care when processing any personal data and only process data on behalf of the Council where such processing is necessary for the Councils business.

You must not disclose this information to unauthorised persons within or external to the Council. This includes discussing confidential matters in public areas. If you have access to personal data, you must use the information for the purposes for which it was gathered only. You must not make copies of personal or confidential data for your own use.

21. Associated Legislation

The relevant UK legislation on which the policy is based include:

- Data Protection Act 2018
- General Data Protection Regulation
- The Computer Misuse Act 1990 (UK)
- Regulation of Investigatory Powers Act 2000
- Defamation Act 1996
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Code of Connection for Government Secure Extranet

For more information on the UK Data Protection Act and GDPR please contact your Information Governance Officer.

22. Responsibilities

This policy will be reviewed annually by the **IT Client Manager** who will:

- Develop and publicise the Council's computer security policies
- Develop administrative, physical, and technical security controls to meet the Council's IT security objectives including allocation of passwords and security of remote access protocols
- Inform all users of any computer security issues
- Conduct periodic audits of Council systems, safeguards and procedures.
- Monitor the use of the internet and email
- Develop appropriate contingency plans to ensure continuity of systems operations
- In co-operation with the relevant Head of Service and Information Governance Officer, perform periodic risk analyses to identify potential information or data losses and the effect of such potential losses.

In consultation with the Joint Chief Executives and representatives from Unison, the recognised Trade Union, this policy will be reviewed regularly by the **HR Client Manager** who will ensure that:

- A copy of this policy is contained within the induction pack issued to new staff
- Induction training courses outline the key elements of this policy, provide general guidance on the use of electronic systems and cross reference with the Council's Equal and Diversity Policy
- IT Support are given a list of starters at least one week before their start date and leavers one week before their last working day so that user information is kept up to date. As a prerequisite a copy of the starters signed acceptance of the current "Internet and Email Users Policy" is required prior to setting up the account.

Heads of Service will ensure that:

- This policy is communicated to all staff, contractors, consultants, and agency staff within their Service area and to all Members
- The procedures within this policy are complied with. Appropriate security measures are established and maintained with regard to access to Council databases and other electronic information systems or resources
- Other than for temporary storage of digital images prior to sifting for permanent storage on the server, Council documents and files must only be stored within O365 OneDrive or SharePoint
- Both Councillors and staff are advised of the importance of maintaining the confidentiality and security of Council documents so that they are not accessible to persons who are not entitled to see them
- No user attempts to remove or disable the Council's virus software from devices in their department, unless authorised by the IT Support or the IT Client Manager
- A risk assessment is conducted on workstations within their department.

All **users** of the system will:

- Be responsible for ensuring that the policies and best use practices contained in this policy are complied with
- You should ensure that if you are accessing or processing personal data, your position in the office is not compromised, so that your PC screen can be viewed by unauthorised personnel or 3rd parties. i.e. they should not be positioned close to windows, facing out to gangways or by openings in doors and walls
- Not leave your PC unattended without locking their system by pressing Ctrl, Alt & Delete and selecting the "Lock Computer" option.

No amount of defences, locks or firewalls can guarantee that confidential information will never leave the system. The most important element of the policy is the principle that everyone is personally responsible for ensuring that the equipment they use for business purposes and the access they grant to information are within the limits set out by the Councils' Senior Leadership Team.

23. Monitoring

All access activity to Council information systems and information assets is logged. This activity can be reviewed to detect unauthorised access attempts or inappropriate use of information systems or for investigation purposes. The Council has the right to monitor your use of IT resources to ensure any risk to its information assets are managed accordingly.

24. Enforcement

The policy is designed to ensure that you use the information systems tools you are provided with in a responsible and efficient manner, ensuring that the Councils reputation is maintained appropriately. Where possible the IT team will implement logical and technical controls to verify compliance with this policy through systematic means including but not limited to business tool reports, internal audits, and feedback to the policy owner.

All breaches of this policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the Council's disciplinary policy and handbook. Any queries relating to this policy should be addressed to your line manager.

25. Document Review

This policy may be modified whenever there are changes to the IT environment, or as the threat level to the IT systems and infrastructure changes. The policy will be reviewed annually.

Appendix A password policy

You are responsible for protecting your passwords. Do not give your password to anyone else, including your manager. Change your password immediately if you suspect that someone else knows it. Choose passwords that are easy for you to remember but difficult for others to guess. You must not leave user accounts logged in at an unattended and unlocked computer.

Passwords must be:

- kept secret and must not be disclosed to others
- not be written down unless the record is stored securely
- changed immediately if it has been disclosed to another individual
- not be saved and option boxes for saving passwords should not be checked (i.e. not ticked).
- be at least 12 characters and be a mix of upper / lower case letters and special characters (such as &%£!)
- a mix of letters and numbers unless there are system constraints
- different from your previous 20 passwords
- If temporary passwords are required these must be changed or deleted as soon as possible.
- Temporary passwords must be conveyed to users in a confidential manner
- Passwords should not be based on the following:

    - Family names, initials, or car registrations
    - Months of the year, days of the week or any other aspect of the date, company names, identifiers, or references
    - Telephone numbers or similar all-numeric groups
    - User ID, username, group ID or other system identifier
    - More than two consecutive identical characters
    - All numbers or letters unless the system requires it.

Appendix B – Key Dos and Don’ts of the IT Security Policy

1. Your device is for you and only you, do not lend or let any non-Council staff use your device.
2. All access to the internet is logged and can be used for audit purposes.
3. Lock your screen when you are away from your device.
4. Save all documents to sharepoint do not download information or files to the machine itself.
5. Exercise due care when processing personal and confidential data.
6. Your work machine is for work, keep personal documents and websites away from it.
7. Keep your password safe and make sure it is sufficiently complex.
8. Your Council email address should not be used for non-business-related purposes
9. You should never respond to spam email if this confirms the Council email address.
10. Do not leave mobile equipment unattended in a public area
11. Do not leave IT assets in the boot of a vehicle for any longer than is necessary
12. Log any security issues with servicedeskruddington@capita.co.uk
    0808 1643093