1. Introduction

1.1 Information is an asset that Rushmoor Borough Council (RBC) ("the Council") has a duty and responsibility to protect. The Council acknowledges its responsibility to its community and business partners, and the expectations placed on it where information is concerned.

1.2 As a local authority, the Council will comply with the procedures and requirements of the Public Service Network (PSN) local public services data handling guidelines along with the Payment Card Industry (PCI), International Organisation for Standards (ISO) and the National Cyber Security Centre (NCSC).

1.3 All information held by the council, in all formats, must be used and stored in a secure manner.

1.4 This Policy is in two parts, the first outlines security procedures covering all aspects of processing information. The second part covers security of IT systems.

1.5 The Policy must be read in conjunction with all other Information Governance Policies, including:

- Data Protection Policy
- Security Incident and Personal Data Breach Policy
- Clear Desk Policy
- Remote Working Policy
- Information Management Policy
- IT Policy

1.6 The Policy applies to all Members and employees of the council, both permanent and temporary who use any form of information, data or computer facilities that are connected to the corporate network or contain corporate data. It also applies to contractors, business partners and visitors, not employed by the council but engaged to work with or who have access to council information, (e.g. computer maintenance contractors) and in respect of any externally hosted computer systems.

1.7 The Policy applies to all locations from which council systems are accessed (including home use). Where there are links to enable non-council organisations to have access to council information, officers must confirm the security policies they operate meet the council's security requirements. A copy of any relevant third-party security policy should be obtained and retained with the contract or agreement.

1.8 Suitable third-party processing agreements must be in place before any third party is allowed access to personal information for which the council is responsible.

1.9 Heads of Service should ensure all staff are aware of and understand the content of this policy.

2 Policy Objectives

The main objectives of this policy are to:

- protect our information and prevent data losses
- protect our ICT systems and information assets from threats that compromise their effectiveness
- ensure that users are aware of and fully compliant with all relevant legislation
- create and maintain, a level of awareness of the need for information security to be an integral part of daily operations, and
- ensure the security of data we share both in transit using encryption and through due diligence on the organisations we share with.

3 Policy Compliance

If any user is found to have breached this policy, they could be subject to Rushmoor Borough Council's disciplinary procedure for employees, termination of work for contractors, and procedures for a breach of the Code of Conduct for Councillors.

Some aspects of information security are governed by legislation, the following are applicable throughout this policy:

- Data Protection Act (DPA) 2018
- General Data Protection Regulation (GDPR) 2016
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Payment Card Industry (PCI) Guidelines governing the taking of electronic payments

Other council policies and procedures may also be relevant such as
Corporate risk management
Health and safety procedures (using mobile phones)

4 Responsibility for security

4.1 Information security is the responsibility of the councils as corporate entities and of all members of staff. A Senior Information Risk Owner (SIRO), supported by the Information Governance Group, has the responsibility for managing the councils' information governance. The SIRO, Leadership Team (LT) and members have approved this information security policy

4.2 All third-party providers of services are responsible for ensuring the security, integrity and availability of information within the service provided.

4.3 All IAOs and IAAs are responsible for the implementation and monitoring of the information security policy.

4.4 **Managers must**:

- be aware of information or portable ICT equipment which is removed from the council offices for the purpose of site visits or home working and ensure staff are aware of the security requirements detailed in section 8 below
- ensure all staff, whether permanent or temporary, are instructed in their security responsibilities
- ensure staff using computer systems/media are trained in their use
- determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status
- ensure staff are unable to gain unauthorised access to council IT systems or manual data
- implement procedures to minimise the council's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas
- ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable
- ensure that the relevant system administrators are advised **immediately** about staff changes affecting computer access (e.g. job function changes leaving business unit or organisation) so that passwords may be withdrawn or changed as appropriate
- ensure that all contractors undertaking work for the council have signed confidentiality (non-disclosure) undertakings

- ensure the council's Clear Desk Policy is enforced, particularly in relation to confidential or personal information. The Clear Desk Policy can be found in Section 11 below.

- ensure information held is accurate, up to date, and retained in line with council retention schedule.

- ensure relevant staff are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments, Data Sharing Agreements to which the council is a signatory and the PSN Acceptable Usage Policy.

4.5 **Members and Staff are responsible for**:

- ensuring that no breaches of information security result from their actions

- reporting any breach, or suspected breach of security without delay. Further details can be found in the Data Breach Policy

- ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.

- ensuring they are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments, Data Sharing Agreements to which the council is a signatory and the PSN Acceptable Usage Policy.

4.6 All staff should be aware of the confidentiality clauses in their contract of employment.

4.7 Advice and guidance on information security can be provided by the Data Protection Officer and, in relation to IT security, the IT Manager.

PART 1 - KEEPING INFORMATION SECURE

5 Data Protection by Design and Default

5.1 The General Data Protection Regulation (GDPR) requires that organisations' put in place appropriate technical and organisational principles and safeguard individual rights. This is known as 'data protection by design and by default'. This means that we must integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle.

5.2 The council will, therefore, ensure that privacy and data protection is a key consideration in everything we do. As part of this we will:

- consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- make data protection an essential component of the core functionality of our processing systems and services
- anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals
- only process the personal data that we need for our purpose(s) and that we only use the data for those purposes

5.3 Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:

- Potential problems are identified at an early stage
- Increased awareness of privacy and data protection
- Legal obligations are met, and data breaches are minimised
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

5.4 Data Protection Impact Assessments (DPIAs) are an integral part of taking a privacy by design approach. Guidance on undertaking a DPIA can be found on the intranet.

6 Data Breaches and Information Security Incidents

6.1 Staff should be aware of requirements in relation to identifying and reporting security incidents and personal data breaches, as set out in the Security Incident and Personal Data Breach Policy

7 Access control

7.1 Staff, Members and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of

staff or contractor is prevented from disclosing information which they had no right to obtain.

7.2 Formal procedures will be used to control access to systems. An authorised manager must raise an IT Service Request for each application for access. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Managers must ensure they advise IT of any changes requiring such modification/removal in a timely manner.

7.3 Staff, Members and contractors must comply with the council's IT Policy in relation to passwords.

7.4 Line managers must ensure that passwords to local systems are removed or changed to deny access when it is no longer needed. This would apply where, for example, the system is externally hosted and not under the remit of IT.

7.5 Where appropriate, staff working out notice are assigned to non-sensitive tasks or are appropriately monitored.

7.6 Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

7.7 Once an employee has left, it can be impossible to enforce security disciplines, even though legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

7.8 System administrators will delete or disable all identification codes and passwords relating to members of staff who leave the employment of the council on their last working day. The employee's manager should ensure that all PC files of continuing interest to the business of the council are transferred to another user before the member of staff leaves.

7.9 Managers must ensure that staff leaving the council's employment do not inappropriately wipe or delete information from any council system. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to council information and equipment.

7.10 All visitors should have official identification issued by the council. If temporary passwords need to be issued to allow access to confidential systems, these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

7.11 There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. IT Services will advise on the most suitable control. They should only have the access rights they need and no more.

7.12 Physical security to all office areas is provided through the access control system. Staff should challenge strangers in the office areas without an ID badge. Never let someone you don't know or recognise to tailgate you through security doors.

8 Security of Equipment

8.1 Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

8.2 Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

8.3 Due to the high incidence of car thefts laptops or other portable equipment must **never** be left unattended in cars or taken into vulnerable areas.

8.4 Users of portable computing equipment are responsible for the security of the hardware and the information it holds on or off council property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

8.5 Staff working from home must ensure appropriate security is in place to protect council equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring council equipment and information is kept out of sight.

8.6 Council issued equipment must not be used by non-council staff.

8.7 All the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the council.

8.8 Users of this equipment must pay attention to the protection of personal data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will refer to the instruction book to learn how to apply these passwords or may plan for basic training in the use of a portable computer.

8.9 Users of portable equipment away from council premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

8.10 Staff and Members who use portable computers belonging to the council must use them solely for business purposes otherwise there may be a personal tax/National Insurance liability.

9 Bring Your Own Device (BYOD)

BYOD refers to any person wishing to use a device owned by someone other than the Council in order to access Council data. The Council can provide access to Outlook

email, contacts and calendar through a secure application on your own device. Please read and adhere to the Remote Working Policy.

9.1 Current devices approved for BYOD are Android phones and tablets, iPhones and iPads. Users must ensure that devices are kept up to date with the latest operating system. Because Android devices are less secure than iPhones and iPads, users are required to have anti-malware software installed on their devices. If this is not installed RBC will deploy anti-malware software onto the user's Android device. As technology improves and newer versions of operating systems are introduced, or vulnerabilities are discovered in existing operating systems then devices should be updated. If not updated, then the device will be deemed as non-compliant and access will be revoked without notice

9.2 Device user responsibilities

- You will not lend anyone your device to access RBC data.
- Should you sell, recycle, or give away your device, you must notify the IT Service Desk immediately. Failure to do so may result in a loss of Council data and may result in disciplinary action.
- You should have a 6-digit pin or fingerprint to access your device. In any event, the user will still have to enter a secure PIN or biometric log on to access the application.
- The application, to access the Council email, is required to automatically lock every 5 minutes of inactivity and will require you to re-enter your pin.
- In order to setup your device to access your work outlook email, calendar and contacts you will need to enter your network account password. You will be required to change this every 90 days.
- You are responsible for the safekeeping of your own personal data and ensuring that it is backed up.
- Any sensitive information should not be emailed via your mobile device, as it will not be secure. A Council owned and managed Laptop or PC should be used.
- You must not use your device to store corporate emails, files or data.
- If any of the following events occur:
  - The device is lost or stolen (which must be reported immediately you become aware)
  - Your employment is terminated without notice
  - You terminate your employment (after your notice period has expired)
  - IT Services detect a data or policy breach or virus,

  IT Services will wipe all Council related data from the device. In so doing, there is a risk that ALL data on the mobile device may be wiped
- All users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, 'jailbreaking' your iPhone or 'rooting' your android device. Any devices that become rooted or jail broken will automatically stop synchronising and will be reported to the IT Service Desk.
- All users must comply with GDPR and Data Protection Act 2018 and Council guidance when using any personal device for work.

9.3 Process for requesting access to BYOD

Requests for BYOD should be made through the IT Service Desk. All relevant policies must be read.

The BYOD software will be installed onto your device. For Android devices if anti-virus software is not on your device then this will be installed at this stage prior to the BYOD software being put onto your device.

10 Payment Card Industry (PCI) Compliance

10.1 The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmit credit or debit card information maintain a secure environment.

10.2 Failure to comply with these standards could lead to fines or even the removal of the Councils ability to accept card payments.

10.3 Those users who have access to any part of the Councils Cash Receipting systems whereby they are taking payments either in person or over the phone should only enter Card numbers into the relevant payment screens and **under no circumstances** should Card Holder data such as Card Numbers be written down or copied by anybody.

11 Security and Storage of Information

11.1 All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT systems
- Computer screens to be ‘locked’ whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for site visits or when working from home) are always to be kept secure and not left in plain sight in unattended vehicles or premises
- Laptops must **never** be left in unattended vehicles

- It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home

- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through the council's network.

- To preserve the integrity of data, frequent transfers must be maintained between portable units and the main council computer system.

- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

12 Remote and mobile working arrangements

12.1 Users should be aware of, and follow, the Remote Working Policy which outlines their responsibilities whilst working away from the normal office environment.

12.2 Whilst working remotely staff, as a minimum, should ensure the secure storage of documents, devices and keep anti-virus and security software up to date on any equipment used to access the council's network.

13 Clear Desk Policy

13.1 Employees are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

13.2 Although security measures are in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

13.3 Employees must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

14 Email

14.1 Email is available to all employees and members. It is accessible from desktop PCs and via the secure Microsoft outlook site. Email is provided to assist in legitimate Council business.

14.2 At **no time** must a redirection or Auto-Forwarding be used from the RBC email to any external email address.

14.3 Non-work email accounts must not be used to conduct or support official Council business. All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

14.4 To ensure work can continue if you were unexpectedly absent or during leave, you should give proxy access to a colleague/Manager. If you have not done this and access is required in your absence, your line manager can request access to your emails. See the Email Policy

15 Posting or Emailing Information

15.1 If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

15.2 Please consider the risk of data breach and the harm or distress that could be caused to the customer if the information is lost or sent to another person, as well as the repercussions for the Council namely reputational damage and possible action by the ICO, when considering the most appropriate way of sending the information to the recipient.

15.3 It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

15.4 Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list. Both options can be found in Outlook under 'file', 'options' and 'mail'
- Take care when replying 'to all' – do you know who all recipients are, do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password e.g. telephone call, messenger or text
- Consider the use of secure email where this is available, or encrypt the document
- Person identifiable data files **must not** be sent via email to a user's personal mail box. Staff working from home should only access information via the council's network.

15.5 Sending information by post:

- Check that the address is correct

- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error

- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Post room, this could be by Special Delivery or even courier.

15.6 Printing and Photocopying:

- All printing must be via the MFP printers

- Consideration must be given to using the Print Room for large print runs, especially where personal information is concerned.

- When printing or photocopying multiple documents, ensure you separate them when you return to your desk

- If the copier jams please remove all documents – if the copier remains jammed report it but leave your contact details on the copier so that once it has been fixed any remaining copying can be returned to you. If possible, cancel your print run

- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run

- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

16 Redacting

16.1 If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used

16.2 The use of black marker pen is **not** a suitable method of redaction

16.3 It is not advisable to change the colour of text (e.g. white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

17 Sharing and Disclosing Information

17.1 When disclosing personal or sensitive information to customers, particularly over the phone or in person, ensure you verify their identity. Service areas dealing with customers daily must have suitable security questions which must always be used.

17.2 If a request for disclosure of information is received from a third party, you must:

- Obtain written consent from the customer that they are acting on their behalf

- Verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.

17.3 In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary. If in doubt contact the Data Protection team for guidance.

18 Retention and Disposal of Information

18.1 Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period. Some information can be retained longer for statistical purposes.

18.2 Staff should refer to the council's Information Retention and Disposal Schedule for further information. The Schedule sets out the type of information held in service areas, together with statutory or agreed retention periods. Please contact the DPO for further advice on retention

18.3 When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the confidential waste bins. Electronic information must be permanently destroyed. Contact IT for advice.

18.4 When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage

18.5 All information destroyed in accordance with the Retention Schedule must be logged on the Disposal log.

19 Vacating Premises or Disposing of Equipment

19.1 It is important that a process is in place to ensure all council information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

19.2 The disposal of computer or other electronic devices is referenced in Section 25 of this policy and all electronic equipment must be returned to IT to be properly disposed of.

19.3 If the council vacates any of its premises, the manager of the service area occupying the premises must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all council information is removed. Such checks should be documented, dated and signed.

19.4 If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

19.5 Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers. If a cupboard or cabinet is locked and no key is available, facilities should be asked to open it in order that it can be checked.

PART 2 – ICT SECURITY

20 Cloud Storage Solutions

20.1 The use of cloud storage solutions (Dropbox, OneDrive Personal, iCloud etc.) for the transfer of council information is expressly forbidden. The IT service can provide you with access to its secure OneDrive for Business for the sharing of files.

21 Systems Development

21.1 All system developments must comply with the council's IT Strategy following NCSC Guidelines. All system developments must include security issues in their consideration of new developments, seeking guidance from the IT Manager and Internal Audit, where appropriate.

21.2 Privacy Impact Assessments (PIAs) should be carried out prior to the purchase of any new system which will be used for storing and accessing personal information.

22 Network Security

22.1 The council will engage a third-party specialist to routinely review network security, this is done by the PSN Health Check.

23 Risks from Viruses

23.1 Viruses (including malware and zero-day threats) are one of the greatest threats to the council's computer systems. PC viruses become easier to avoid with staff and members aware of the risks with unlicensed software or bringing data/software from outside the council. Anti-virus measures reduce the risks of damage to the network.

23.2 IT Services centrally maintain and update the currency of the virus definition files on servers, but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support is available from IT Services if any remedial action is necessary. Any suspected virus attacks must be reported

23.3 Anti-virus guidelines can be found at Appendix 1.

24 Cyber Security

24.1 Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day to day operations of the council, the delivery of local public services and ultimately have the potential to compromise national security.

24.2 The council's approach to cyber security can be found in Appendix 2.

25 Access Control to Secure Areas

25.1 Secure areas include:

- The post room
- The ICT server room

25.2 All central processors/networked file servers/central network equipment will be in secure areas with restricted access.

25.3 The council's central computer suite is a high security area housing corporate computer systems. Entry restriction and detection systems are in place to protect the suite.

25.4 Local network equipment/file servers and network equipment will be in secure areas and where appropriate within locked cabinets.

25.5 Unrestricted access to the central computer facilities will be confined to designated staff whose job function requires access to that area/equipment.

25.6 Restricted access may be given to other staff where there is a specific job function need for such access.

25.7 Authenticated representatives of third-party support agencies will only be given access through specific authorisation.

25.8 All secure areas will have an entry log which staff and visitors must use.

25.9 Regular reviews of who can access these secure areas should be undertaken

26 Security of Third-Party Access

26.1 No external agency will be given access to any of the council's networks unless that body has been formally authorised to have access.

26.2 All external agencies will be required to sign security and confidentiality agreements with the council.

26.3 All external agencies processing personal information on the council's behalf (including via a hosted IT system) will be required to sign a third-party processing agreement.

26.4 The council will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

26.5 The council will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request

confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

26.6 All third parties and any outsourced operations will be liable to the same level of confidentiality as council Staff.

27 Data Back-up

27.1 Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive without the approval of the IT Manager.

27.2 Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

27.3 IT Services and all other systems administrators should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this back-up. A cyclical system, whereby several generations of backup are kept, is recommended.

27.4 Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The council's Retention Schedule must be followed in determining whether data should be archived.

27.5 Recovery data should be enough to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

27.6 To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.

27.7 Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.

27.8 If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

28 Equipment, Media and Data Disposal

28.1 If a machine has ever been used to process personal data as defined under the Data Protection Act (2018) or 'in confidence' data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented on the council's disposal log.

28.2 Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

28.3 Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software. Therefore, disposal must be arranged through IT Services who will arrange for disks to be wiped or destroyed to the appropriate standards.

29 Software

29.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

29.2 The loading and use of unlicensed software on council computing equipment is **NOT** allowed. All staff and members must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. The council monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the council's Disciplinary Procedure

29.3 The council will only permit authorised software to be installed on its PCs. Approval will be via IT Services.

29.4 Where the council recognises the need for specific specialised PC products, such products should be registered with IT Services and be fully licensed.

29.5 Software packages must comply with and not compromise council security standards.

29.6 Computers owned by the council are only to be used for the work of the council. The copying of leisure software on to computing equipment owned by the council is not allowed. Copying of leisure software may result in disciplinary action under the council's Disciplinary Procedure. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

29.7 Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by IT Services staff or its authorised representatives. Where a software training package includes 'games' to enable the new user to practise their keyboard skills e.g. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

29.8 The council seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to IT Services. **See appendix 1 for the Anti-Virus guidelines.**

29.9 Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact IT Services for anti-virus advice.

30 Use of Removable Media

30.1 It is the council's policy to prohibit the use of all unauthorised removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed.

30.2 All staff, Members and third parties must comply with the requirements regarding removable media which can be found in the IT Policy

31 Timeout Procedures

31.1 Inactive computers should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also close both application and network sessions. A high-risk area might be a public or external area outside the control of council security management. The time-out delay should reflect the security risks of the area.

31.2 Users must 'lock' their computers, if leaving them unattended for any length of time. For high risk applications, connection time restriction should be considered. Limiting the period during which the computer has access to IT services reduces the window of opportunity for unauthorised access.

32 System Documentation

32.1 All systems should be adequately documented by the system manager and should be kept up to date so that it always matches the state of the system.

32.2 System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.

32.3 Distribution of system documentation should be formally authorised by the system manager. System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.

32.4 Manual data covered by the PSN must not be removed from the council offices in accordance with the agreement.

32.5 General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems.

This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore, care must be taken when transferring data between your home PC and the council network. All home PCs which are used for the manipulation of council data must have a current virus checker with up to date virus signatures.

APPENDIX 1 - Anti-Virus Guidelines

1. What is a virus?

A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There are currently something like 60-75,000 known viruses and worms [1] - some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates.

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

2. What does the council's IT Services do to prevent the spread of viruses?

Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators, security officers, and anti-virus software. The best efforts of administrators and security experts are not enough - all computer users must also play their part by taking simple precautions like those described below.

3. Avoid Unauthorised Software

Programs like games, joke programs, cute screensavers, unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden to install them. If such programs are claimed to be some form of antivirus or anti-Trojan [2] utility, there is a high risk that they are in some way malicious!

4. Treat all attachments with caution

It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know, don't assume they must be OK because you trust the sender.

---

[1] A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

[2] In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

Worms generally spread by sending themselves without the knowledge of the person from whose account they spread. If you do not know the sender or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply.

However, one recent virus sends out an email telling you that a 'safe' attachment is on the way, then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with suspicion:

- If they come from someone you don't know, who has no legitimate reason to send them to you.
- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).
- If it concerns unusual material like pornographic websites, erotic pictures and so on.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice" or "I love you!").
- If the attachment has a filename extension that indicates a program file (such as those listed below).
- If it has a filename with a 'double extension', like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a text file or JPEG (graphics) file.

In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question.

5. Avoid unnecessary macros

If Word or Excel warn you that a document you're in the process of opening contains macros [3], regard the document with particular suspicion unless you are expecting the

[3] In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

document and you know that it's supposed to contain macros. Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

6. Be cautious with encrypted files

If you receive an encrypted (passworded) attachment, it will normally be legitimate mail from someone you know, sent intentionally (though the sender is unlikely to know if they have a virus). However, that doesn't necessarily mean that it isn't virus infected. If it started out infected, encryption won't fix it. Furthermore, encrypted attachments can't usually be scanned for viruses in transit: the onus is on the recipient to be sure the decrypted file is checked before it's opened. This goes not only for heavyweight encryption packages, but also for files compressed and encrypted with PKZip or WinZip.

7. Suspicious filename extensions

The following is a list of filename extensions that indicate an executable [4] program, or a data file that can contain executable programs in the form of macros. This list is by no means all-inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort.

Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with the filename extension .ZIP can contain one or more of any kind of file.

.BAT	.CHM	.CMD	.COM	.DLL	.DOC	.DOT
.EXE	.FON	.HTA	.JS	.OVL	.PIF	.SCR
.SHB	.SHS	.VBS	.VBA	.WIZ	.XLA	.XLS

8. Report it!

If you think that you may have received a virus - report it!

[4] An executable is a file that contains a program. It is a particular kind of file that is capable of being executed or run as a program in the computer. In a Windows operating system, an executable file usually has a file name extension of .bat, .com, or .exe.

APPENDIX 2 - Cyber Security Approach

1. Introduction

This document identifies the risks to the council from main threats of cyber security and sets out what is in place to mitigate these risks.

If you do not understand anything in this document or feel you need specific training you should bring this to the attention of your line manager.

2. Purpose and Objectives

The document provides guidance to staff and members on the risks that threats from cyber security pose to the council.

In addition the following policies are relevant to all staff and have some impact on the threats from cyber security:

- IT Policy
- Information Management Policy
- Home & Remote Working Policy

3. Roles and Responsibilities

The IT Manager is responsible for the provision of the appropriate technology and technological devices to ensure that the council is reasonably protected from the threats from cyber security.

The council is responsible ensuring that staff are communicated with about how to ensure that they don't put the council at risk.

All employees, contractors and members should not take any action that puts the councils systems or information at risk from cyber security. Any incidents must be reported in line with the Information Security policy.

4. Cyber Security

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the council, the delivery of local public services and ultimately have the potential to compromise national security. Additional costs will be incurred by the council to rectify any cyber security or cybercrime event.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

The scale of targeted attacks coupled with the difficulty of monitoring all possible attack methods requires the public sector to work together to both reduce the likelihood and the impact of such a threat succeeding.

Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives that include:

- Stealing sensitive information to gain economic, diplomatic or military advantage over the UK
- Financial gain
- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure

Council employees can also be targets for criminal activity.

5. Cyber Security Risks

The following types of cyber security all pose risks to the council:

- Cybercrime:

  The most common form of cyber-attack against public bodies is the use of stolen or false customer credentials to commit fraud.

  The uptake in online services means this form of crime can now be undertaken on a much larger scale and can be international.

  Cybercriminals also seek to steal data from government networks that has a value on the black market, such as financial information or data that can be used for ID theft.

  There are several types of malware (malicious software) that have been written to specifically steal banking and log in information.

  The council secures its network with up to date antivirus and malware protection, and manages the use of personal USB devices on council computers.

- Hacktivism:

  Hacktivists seek to cause embarrassment or annoyance to the owners of high-profile websites and social media platforms that they may deface or take off line.

  When targeted against local government websites and networks, these attacks can cause reputational harm both locally and nationally.

  The council has third party availability monitoring tools in place to alert key team members of the websites status.

  The council's web site's content management system conforms to the councils ICT Policy with regards to password enforcement.

- Insider threats:

  An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include:

  - Unauthorised disclosure of sensitive information
  - Facilitation of third-party access to an organisation's assets
  - Physical sabotage
  - Electronic or IT sabotage

  Not all insiders deliberately set out to betray their organisation. An unwitting insider may compromise their organisation through poor judgment or due to a lack of understanding of security procedures.

  The insider threat is not new, but the environment in which insiders operate has changed significantly. Technology advances have created opportunities for staff at all levels to access information.

  The council enforces the use of strong passwords for access to systems.

  The council only allows corporate USB devices to be written to. All personal USB devices are read only.

  The council uses mobile device management tools to secure corporate information on personal devices (smart phones and tablets).

  The council periodically reviews access to key IT systems.

- Physical Threats:

  The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that could impact upon local government IT systems.

  The council has a disaster recovery (DR) and business continuity (BC) data centre for its high impact services. It also has a shared telephony platform with Hart District Council with DR / BC built in.

- Terrorists:

  Some terrorist groups demonstrate intent to conduct cyber-attacks, but have limited technical capability. Terrorist groups could acquire improved capability in a number of ways, namely through the sharing of expertise in online forums providing an opportunity for escalations and the hiring of Hacktivists.

- Espionage:

  Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations.

6. The council's approach to Cyber Security

As with most local authorities, the council relies heavily on access to the internet and to information held in its systems. There are several IT systems that have an internet presence (website, webmail homeworking), and there are several different access mechanisms to information (Wi-Fi, physical networking, smartphones, tablets). All present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all the time, but the council employs a range of tools and good practice to minimise the risk to its information and systems.

The council has clear polices on ICT and Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Passwords
- Removable Media
- Clear desk policy
- Sharing and disclosing information
- Cloud storage systems
- Viruses
- Equipment, media and data disposal

The council implements security controls and good practice to enable it to achieve compliance with Payment Card Industry Data Security Standards (PCI DSS) and Public Services Network (PSN). Both require the council to ensure that systems are security patched and that the council has regular penetration tests of its network/systems that are performed by a third party.

The council employs a range of technology and processes to help it achieve a good security platform. These range from up to date firewalls and core networking equipment, through antivirus controls and a secure wireless configuration, to encrypted devices, two factor authentication and mobile device management. The council also subscribes to the Cyber-security Information Sharing Partnership (CiSP) which is part of the NCSC.

7. Communications-Electronic Security Group (CESG)

CESG is part of GCHQ and aid government departments on information security and assurance.

CESG has published a document detailing 10 Steps to Cyber Security, these are listed below along with the steps that the council has adopted to mitigate the risks.

Information Risk Management Regime. The information governance team manages information risk proactively through the council's Information Management Policy which provides information to staff and members about information retention and disposal and information sharing. The team works with service areas to help them design and implement regimes for their information.

Secure Configuration. The council's IT service has default build processes for corporate devices and ensures that operating systems, services and applications are patched against known vulnerabilities. All corporate computers and servers are inventoried. Servers and network environments log activities for auditing purposes.

Network Security. The IT service manages a number of tools sets to ensure network security; these are periodically reviewed to ensure they meet security and business needs. The security configuration is also reviewed annually as part of the council's PSN submission. Internal and external network access is regularly tested by third party security consultants.

Managing User Privileges. The IT service manages core systems and applications. User logins for computers are managed by the IT service and access to information must be requested by a manager through an IT Service Request. Access to corporate applications is managed by the IT service and permissions granted in line with job requirements. Wherever possible user activity is logged, access to activity logs is restricted to IT System Administrators and Internal Audit.

User Education and Awareness. The IT service and the Information Governance team periodically send emails and information about threats to the organisation. Policies and mandatory eLearning are in place.

Incident Management. The council has processes and recovery places for disaster recovery and business continuity. These are managed by the IT service and collated centrally within the Finance and Resources Directorate. There are also processes in place for the reporting and response for information and security incidents.

Malware prevention. The IT Service manages the council's antivirus and malware solutions. Signatures for malware and antivirus are updated automatically on all corporate computers.

Monitoring. The IT Service logs all system and security events across its server environment and has software in place to alert for internal and external threat attempts. The council subscribes to Cybersecurity information Sharing Partnership (CiSP), part of NCSC, for third party alerting and expertise.

Removable Media Controls. The IT service has implemented a solution to manage USB devices on corporate devices, ensuring that only approved and encrypted devices can be written to.

Home and Mobile working. The IT Service employs several tools to ensure security of information for home and mobile working, including Mobile Device Management solutions to encrypt corporate mobile devices and corporate information on personal devices. Additionally the council uses two factor authentication for access in webmail and home working portals. Information transported over virtual private networks (VPN's) is encrypted.