11. ICT ACCEPTABLE USE POLICY

1 Purpose

1.1 The main purpose of this policy is to ensure that Rushmoor Borough Council's name is not bought into disrepute or its reputation, customer relations, or public image adversely affected by ensuring that data is held securely, used appropriately and any inappropriate use of Council equipment is prevented.

1.2 The policy also ensures that the Council and users meet legislative requirements, including Government Connect Code of Connection.

Giving access

2.1 All employees, Members and workers will be given this Policy.

2.2 All employees, including Members and Temporary staff and workers e.g. work experience, volunteers or contractors, are required to sign a copy of the declaration, attached at the end of this policy. By signing the declaration, they agree that they have read and will abide by the requirements of the AUP.

2.3 Line managers should advise the IT Service Desk of the need for access for an employee within a reasonable time prior to the access being needed. The IT Service Desk will require the following information:

- Name
- Department
- Job title
- Access to which systems
- Access level required for all of the systems

2 Removing/Changing access

3.1 A request, to remove access for staff or where a change in duties occurs, should be made by the Line Manager to the IT Service Desk where possible within 2 weeks of when the change is required.

3.2 Before an employee leaves the Council, they should ensure data stored on their U: drive is transferred to an area colleagues can access e.g. the S: drive. When the person leaves, their network account will be suspended. Data will be held for a further month, but access will only be available through IT Services. After the month has passed, data will be deleted from the network and therefore irretrievable.

3.3 Should access to emails from employees who have left be required, requests from line managers should be made to the IT Service Desk. The emails will still be held within the Email archive for the applicable time as per the email policy for retention.

3 Passwords

4.1 Passwords are the first line of defence for our ICT systems and together with the username, they 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.

4.2 Weak passwords are ones which, for example, include words picked out of a dictionary. A strong password is one which 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. Therefore, strong passwords should be used, i.e.:

- At least seven characters
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word otherwise they would be easy for hackers to crack

4.3 Passwords can be used on individual electronic files such as word and excel. However, it is important to remember these passwords, as IT Services are unable to unlock the file if you forget the password used.

4 User responsibility

5.1 It is of utmost importance that a user's password remains protected at all times. Note the following:

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

5.2 Default passwords must be changed immediately. If a user becomes aware, or suspects, that their password has become known to someone else, the user must change it immediately and report any concerns to the IT Service desk.

5.3 It is a user's responsibility to prevent their username and password being used to gain unauthorised access to Council systems by:

- Ensuring that any PC they are using is locked or logged out when left unattended so that the user cannot be held responsible for someone else's actions.
- Leaving nothing on display that may contain access information such as login names and passwords

5 Physical Security

6.1 Access to the Council offices and the IT Data Centre is controlled by a swipe card system. The card doubles as ID and if lost must be immediately reported to the Facilities Team. All visitors to the Council offices must report to the main reception and sign in.

6.2 Security pass activated doors should not be propped open and any unknown person following a card holder through security doors should be approached to confirm they are legitimate visitors.

6.3 Portable IT equipment must be held securely while in the office and locked away when not attended.

6.4 Users should ensure that all sensitive data is cleared from their desk when they are not using the data. Sensitive personal data in paper format must be locked away when unattended, and only authorised people should have access to it in order to conform to the Data Protection Act 1998.

See also guidance on the Data Protection Act. – http://inform/StaffHandbook/communications/dataprotect.htm

6.5 To carry out business it may be required to take personal data out of the Council Offices either in paper format or on a portable device. When doing this:

- Only take the information needed
- Do not leave it unattended
- Do not leave it on view in a locked car.

6 Health and Safety

7.1 It is the policy of Rushmoor Borough Council to provide a safe and healthy working environment for employees, including particular measures to protect their health and safety when they are working. Please see http://inform/StaffHandbook/health/healthsafetypolicy.htm for guidance relating to Health and Safety within Rushmoor.

7 Using the Internet

8.1 The Internet is a useful tool to enable users to carry out their daily work activities. However, an Internet policy is in place and should be adhered to. Below is a summary of key points from the Internet policy:

- Users must familiarise themselves with the detail of the Internet policy before using the Internet facility provided.
- The Council's internet access is primarily for business use. However, reasonable personal use is permitted in an officer's own time providing it does not interfere with work.

- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other ‘unsuitable’ material that might be deemed illegal, obscene or offensive.
- Monitoring software is in place to automatically block access to specific categories of websites, for example, gambling.
- The data collected through monitoring will be used to ensure compliance with the Internet policy.
- Software must not be downloaded onto Council equipment.
- Access to social networking sites is restricted to those officers who require it for their job. A request for access can be made to IT. Each request requires a business case supported by the Head of Service outlining why and for what period access is required.

8 Email

9.1 Email is an effective form of communication. However, an email policy is in place and should be adhered to. Below is a summary of key points from the policy however, please see Inform for the detailed Email policy:

- All emails that are used to conduct or support official Council business must be sent using a ‘@rushmoor.gov.uk’ address. Non-work email accounts must not be used.
- For users of GCSx, all emails sent via the Government Connect Secure extranet (GCSx) must be of the format ‘@rushmoor.gcsx.gov.uk’.
- User should not communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council’s internal Equal Opportunities code of practice.
- The legal status of emails is similar to any other form of written communication. They can be legally binding and used as evidence in court proceedings.
- For users of GCSx automatic forwarding of email must be considered carefully to prevent PROTECT and RESTRICTED material being forwarded inappropriately.
- Monitoring software automatically filters emails for inappropriate or offensive materials.
- To avoid disclosing personal data where you are sending out a group email and you are not sure if they are business email addresses you should blind carbon copy all the recipients. If you require help with this, please contact the IT Service Desk.
- Users should endeavour to avoid sending unnecessary messages using the ‘All’ email facility.

9 Data Sharing

10.1 The term ‘data sharing’ refers to the disclosure of personal data from one or more organisations to a third-party organisation or organisations, or the sharing of personal data between different parts of the organisation.

10.2 If a department requires personal information from another department in order to carry out its own statutory requirements then the data can be shared under Section 35 (1) of the Data Protection Act. Further details with regards to Data Sharing can be found on Inform.

10.3 Where information is requested regarding an account with someone's personal details on, staff should ensure that they have asked relevant security questions to establish that the person speaking is the person whose details they want to discuss.

10.4 When sharing data regularly with external organisations a written pre agreed protocol should be in place and followed. For ad hoc data sharing a request should be made via the Data Protection Officer.

10.5 The Data Protection Act principles must be followed when sharing data, but before sharing data, you should ask yourself the following questions:

- What is the sharing meant to achieve?
- What information needs to be shared?
- Who requires access to the shared personal data?
- When should it be shared?
- How should it be shared?
- What risk does the data sharing pose?
- Could the objectives be achieved without sharing the data or by anonymising it?

10.6 The Council participates in the National Fraud Initiative, which matches electronic data within and between public and private sector bodies to protect and detect fraud. This involves the Council providing the Audit Commission with the details of employees and members from the Council's payroll system.

10.7 For further detail and guidance on data sharing please see the data sharing policy on Inform.

10.8 For employees using the Government Connection scheme please see GCSx Acceptable Use Policy on Inform for additional guidance on GCSx data sharing.

10 Data held on the network

11.1 Storing data on the Council's network is expensive and therefore only work-related data is to be stored on the network. The storage of non-work data is not permitted. If non work data is identified on the network, you will be asked to remove it. If it is not removed, then it may be deleted by your manager or IT to free up space.

11.2 To ensure that valuable space is not taken up on the network indefinitely, users should only hold data inline with the Council's data retention guidelines. http://inform/StaffHandbook/communications/freedominfo.htm

11 Government Connect Secure extranet AUP

12.1 Employees using Government Connect are required to read, accept and sign the GCSx Acceptable Use Policy which can be found on Inform http://inform/StaffHandbook/it/auppolicy.htm This additional security introduces stringent controls on the particularly sensitive data used in this area.

12 Security Incident

13.1 A security incident is an event that has or could result in the loss of or damage to the Council's information. It is also an action that is in breach of the Council's security policies and procedures.

13.2 Please see the Security Incident Policy on Inform for the detailed Security Incident policy, which should be adhered to. However, below is a summary of key points:

- All staff should report any electronic security incidents or suspected incidents immediately to the Head of IT or the IT Technical Services Manager. For example, loss of a USB stick with data held on it.
- All staff should report any paper incidents or suspected incidents immediately to their Head of Service and the Data Protection Officer. For example, leaving personal paper documents on a train.

13 Remote Working

14.1 A summary of the key points in the Remote Working Policy, which should be adhered to, is set out below:

- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- Users should be aware about carrying out adequate health and safety assessments especially when working at different location/desks.
- It is the GCSx users responsibility to ensure that access to all PROTECT or RESTRICTED information is controlled – e.g. through password controls.
- All data held on portable computer devices must be encrypted.

14 Purchasing Software and Hardware

15.1 All IT equipment and software must be purchased through IT services. The reasons for this are that IT Services:

- Will help to identify the best solution for the job.
- Ensure all hardware and software is compatible
- Check to see if they can offer on-going support.
- Ensure it is correctly licensed.
- Can take a business case for the IT equipment to the ICT group for them to review and assess.

15.2 Technical support will not be available for hardware or software not purchased through IT services (and in line with the ICT strategy). In addition, the equipment will not be able to be used in conjunction with Council systems.

15.3 The use of software on the network is continuously monitored. If unlicensed software is identified on an employee’s PC, they will be given 5 working days to either produce a valid licence or remove it. If after that time, it is still in use and a licence has not been produced, IT services will remove the software directly.

15 Removable Media (USB, SD Cards, CDs)

16.1 A summary of the key points in the Removable Media Policy which should be adhered to is set out below:

- Any removable media device that has not been supplied by IT Services must not be used. If they are used on Council equipment, then they will be restricted to read only.
- All data stored on removable media devices must be encrypted.
- Damaged or faulty removable media devices must not be used.
- Special care must be taken to physically protect the removable media devices and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the devices and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Should removable media be lost or stolen please refer to the Security incident policy for the steps to be followed.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage.

16 Instant Message

17.1 Instant messenger is available on desk top PCs. It provides a system for the IT Service Desk to remotely access your PC and give support on technical problems.

17.2 The use of instant Messenger for personal use during work time is discouraged. However, it is recognised that, as with telephone calls, a certain amount of private usage is acceptable, but this is monitored. Private use must be kept to a minimum and not interfere with work.

17 Telephones/Mobile phones/Smartphones

18.1 Office phones are provided to assist the business of the Council. Personal calls are allowed in work time, but must be kept to a minimum, not interfere with work and in the main kept to local calls.

18.2 The Council provides mobile phones to employees who require them to carry out their work. A limited number of personal calls can be made on work mobile phones but calls to premium lines are not permitted. The Council's reputation must be considered when making use of the phone, for example content of texts or photos. Please see the Mobile Phone Policy for further details.

18 Printers

19.1 Door entry cards are activated by the IT Service Desk and enable use of the Council's printers/photocopiers. If a job is sent to the print queue but not printed out within 24 hours, the print job will automatically be deleted. Use of the printers/ photocopiers should be for work purposes only.

19.2 Temporary door entry cards can be obtained from reception and can be activated for use by the IT Service desk for printing/photocopying.

19.3 For queries please contact the IT Service Desk or see the printer page on inform for further details.

http://inform/StaffHandbook/it/docs/printersandcopiershintsandtips.pdf

19 Radios

20.1 When using the Council's radio system, it is not permitted to transmit personal or confidential information, or details that may put officers at risk. The radio is an open system with all broadcasts heard by others with a radio. People who have radio receivers can easily listen to broadcasts.

20.2 The Telecommunications Agency continuously monitor broadcasts to ensure the conditions of the licence are being met, such as only broadcasting appropriate material. If the conditions are breached, then the licence can be withdrawn.

20 Backing up of data

21.1 Work should not be saved to the PC's hard drive (the C: drive). This is not backed up and should the PC fail, the data will be lost. Instead, work should be saved to a network drive that is automatically backed up by IT Services every night.

21 Legal Responsibility

22.1 The following legislation is applicable throughout this policy:

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 1998
- Health & Safety (display screen equipment) regulations 1992 (as amended)

22 Other related council policies and procedures

23.1 Related policies and procedures include:

- Disciplinary procedure
- Code of conduct for Councillors
- Corporate risk management
- Road safety procedures (using mobile phones)

23 Policy Compliance

24.1 If any user is found to have breached this policy, they may be subject to Rushmoor's disciplinary procedure for employees, termination of work for contractors, and procedures for a breach of the Code of Conduct for Councillors. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender.