



ASH-CUM-RIDLEY PARISH COUNCIL INFORMATION TECHNOLOGY POLICY

1. INTRODUCTION	2
2. PURPOSE	2
3. SCOPE	2
4. MONITORING OF IT USE	2
5. COMPUTER USE	2
6. PORTABLE EQUIPMENT	2
7. USE OF OWN EQUIPMENT	3
8. HEALTH AND SAFETY	3
9. PASSWORD AND AUTHENTICATION	3
10. MONITORING	4
11. REMOTE WORKING	4
12. EMAIL	5
13. USE OF INTERNET	5
14. DATA PROTECTION	5
15. SOCIAL MEDIA	5
16. MISUSE	5

1. Introduction

1.1 This policy sets out how councillors, staff, and authorised users must use the council's IT systems and equipment.

2. Purpose of the IT Policy

2.1 The purpose of this IT policy is to ensure the secure and appropriate use of the council's IT systems, protect council data and assets, define acceptable use, and reduce the risk of cyber incidents.

3. Scope

3.1 This policy applies to all councillors, staff, and authorised users, whether working in the office, remotely, or using council systems in any capacity.

4. Monitoring of IT Use

4.1 The council has the right to monitor the use of its IT equipment and systems where there is a legitimate reason to do so. Councillors, staff, and authorised users will be informed that such monitoring may take place.

4.2 Any monitoring will be proportionate and carried out in accordance with relevant data protection and privacy laws. This may also apply to other individuals who access or use council systems, such as those with a council email account.

5. Computer use - Hardware

5.1 Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the clerk. Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

5.2 Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

5.3 All computer and other electronic equipment supplied should be treated with good care at all times.

5.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

5.5 Equipment should not be dismantled or reassembled without seeking advice.

5.6 Only authorised equipment and software may be used.

5.7 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the clerk.

5.8 Any faults or necessary repairs must be reported to the clerk.

6. Portable equipment

6.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

6.2 Council data should be stored on approved cloud-based systems where it is automatically backed up and secured. Users must ensure that work is saved to the council's cloud systems as soon as possible and not retained on local devices longer than necessary. Portable devices must not be relied upon as the primary storage location for council data.

6.3 Council equipment may be taken off-site (e.g. working from home), provided it is used securely and in accordance with this policy. Equipment must remain under the user's control at all times when off-site. Devices must not be left unattended in public places. When travelling, equipment must be kept secure and out of sight. Devices must not be left in vehicles unless unavoidable and only for short periods

6.4 Personal devices used to access council email must be secured with a PIN, password, or biometric protection. Users must take reasonable steps to protect council data and

prevent unauthorised access. Where possible, additional security features such as remote locking or wiping should be enabled.

- 6.5** Multi-Factor Authentication (MFA) is implemented to enhance the security of council email accounts. Users are required to complete MFA when accessing council systems from a new device or location. Trusted devices may retain access following successful authentication. MFA helps protect against unauthorised access and is a key part of the council's information security controls.
- 6.6** If an item of portable equipment is lost or damaged this should be reported to the clerk.
- 6.7** Care must be taken when taking photographs, videos or recordings in council offices. Confidential information or non-public discussions must not be recorded or shared without appropriate permission.
- 6.8** Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).
- 6.9** In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the clerk

7 Use of own equipment

- 7.1** The council recognises that councillors and authorised users may access council email and systems using their own devices.
- 7.2** Such use is permitted provided that reasonable steps are taken to maintain security.
- 7.3** Personal devices used to access council systems must be protected by a PIN, password, or biometric security. Council email accounts must be used for council business, not personal email accounts.
- 7.4** Users must take care to ensure that council information is not accessed by unauthorised persons (e.g. family members or others using the device). Devices should be kept up to date with software and security updates.
- 7.5** Access to council systems must be through secure connections wherever possible. Any loss, theft, or suspected compromise of a device that may contain or access council data must be reported promptly.
- 7.6** Council data should be stored on the council's approved cloud systems and not retained on personal devices longer than necessary. Users should take care to keep council data separate from personal data where possible.
- 7.7** The council reserves the right to take appropriate steps to protect its data where there is a security or legal requirement.

8 Health and safety

- 8.1** Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.
- 8.2** The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the council's health and safety policy.
- 8.3** Users who regularly work with display screen equipment (such as computers or laptops) who feels that their workstation requires changes to make it compliant must speak to the clerk.
- 8.4** If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the clerk.

9 Password and Authentication

- 9.1** All user accounts must be protected by strong and secure passwords. Users are responsible for ensuring that their passwords are kept confidential and not shared with others. Any default passwords must be changed as soon as possible. The council uses

Multi-Factor Authentication (MFA) to enhance security. Users are required to complete MFA when accessing council systems from a new device or location. Once a device has been authenticated, access may continue on that device. MFA helps reduce the risk of unauthorised access to council systems and data.

- 9.2** Access to council systems is restricted to authorised users only. Administrative access, including access to systems such as Microsoft 365, is limited and managed by the Clerk. This level of access must only be used where necessary for council business and handled with appropriate care. Where possible, a basic record of administrative access should be maintained. Administrative credentials must be stored securely and not shared.
- 9.3** Passwords must not be stored in an insecure manner. Users must take reasonable steps to ensure passwords are protected at all times. If a password is suspected to have been compromised, it must be changed immediately. The use of password managers is encouraged where appropriate, but it is not a mandatory requirement.
- 9.4** All users are responsible for maintaining secure access to their own accounts and for following this policy. The Clerk is responsible for managing system administration, including user access and overall access control. Where necessary, the council may seek support from its IT provider to assist with system security and administration.

10 Monitoring

- 10.1** The council reserves the right to monitor the use of its IT systems where necessary to ensure security, proper use, and compliance with this policy. This may include reviewing email usage, system activity, or files stored on council systems where there is a legitimate reason to do so, such as investigating a fault, a suspected breach, or protecting council data.
- 10.2** Monitoring will be carried out in a proportionate and lawful manner, and only where it is necessary. The council does not routinely monitor all user activity, but may review usage if concerns arise or as part of system maintenance and security. Information obtained through monitoring will only be accessed by authorised persons and will only be used for legitimate purposes. It may be shared internally where required, or with professional advisers where appropriate. Any information gathered will be retained only for as long as necessary and handled in accordance with the council's Data Protection Policy. Users have rights in relation to their personal data, including the right to request access, in line with data protection legislation. Any misuse of council IT systems may result in appropriate action being taken.
- 10.3** The council relies on its cloud-based systems and service providers to support system security and monitoring where appropriate.

11 Remote working

- 11.1** Increased care must be taken when accessing council systems or handling council information away from the usual place of work, including when working from home or in other locations.
- 11.2** Users must ensure that council information remains secure at all times. Devices should only be used in a secure environment and must not be left unattended in public places. Screens should be positioned to prevent confidential information from being viewed by others.
- 11.3** When accessing council systems on devices that are not owned by the user or the council, passwords must not be saved and users must log out fully after use. If a device cannot be used securely, council systems should not be accessed from it.
- 11.4** Any council documents, whether electronic or printed, must be handled carefully and stored securely. Printed documents should not be left unattended and should be disposed of securely when no longer required.

- 11.5** Council data should be saved to the council's approved cloud systems wherever possible and not retained on local devices longer than necessary.
- 11.6** Where available, device security features such as screen locks, updates, and remote locking or wiping should be used.
- 11.7** Access to the internet in public locations should be undertaken with caution, and users should ensure they are using secure connections wherever possible.

12 Email

- 12.1** Council email accounts are provided for official council business only and must be used in a professional and responsible manner.
- 12.2** All councillors, staff, and authorised users who require email access will be provided with a council email account. Council business must be conducted using this account rather than personal email addresses.
- 12.3** Users must remain vigilant to potential security risks, including phishing emails and malicious attachments, and should not open suspicious messages or links. Any concerns should be reported to the Clerk.
- 12.4** Email access may be withdrawn where it is no longer required for a user's role or where misuse is identified.

13 Use of the Internet

- 13.1** The council requires all councillors, staff, and authorised users to comply with copyright laws when using material obtained from the internet or other sources. Users must not copy, download, or use material unless they are permitted to do so. Care should be taken to ensure that any content, including documents, images, or software, is used lawfully and appropriately. If there is any uncertainty about whether material can be used, advice should be sought from the Clerk.
- 13.2** This includes the use of Artificial Intelligence (AI) tools and services, which must be used in accordance with this policy.

14 Data protection

- 14.1** The handling of personal data must comply with the council's Data Protection Policy. All councillors, staff, and authorised users must ensure that personal and sensitive information is managed appropriately.
- 14.2** This includes ensuring that personal or sensitive data is not entered into unauthorised Artificial Intelligence (AI) systems and is only used within approved and secure environments.

15 Use of Artificial Intelligence (AI)

- 15.1** Approved AI tools are those authorised by the Council and provided within the council's secure IT environment (currently including Microsoft 365 Copilot). Public or unapproved AI tools (for example ChatGPT, Claude or Google Gemini) must not be used for council information (including Ash Green Sports Centre) unless authorised by the Clerk.
- 15.2** Users must not input confidential, personal, commercially sensitive or legally privileged information into AI tools unless it is necessary for council work and the system is approved and secure. Where personal data is used, only the minimum necessary information should be included. Any outputs containing personal data must be handled appropriately and only shared where necessary.
- 15.3** AI tools may be used to summarise emails, documents, and other information. However, all AI-generated content must be checked for accuracy, completeness, bias and appropriateness before use. Users remain responsible for any content produced using AI.

15.4 AI must be used as a support tool only and must not replace professional judgement, decision-making, or statutory responsibilities. Use must comply with the council's Data Protection Policy, copyright requirements, and standards of conduct, and must not mislead, misrepresent, or compromise the council's integrity or reputation.

15.5 Any concerns or uncertainty regarding the use of AI should be referred to the Clerk.

16 Social Media

16.1 The council uses social media as a means of communication with the public. Official council social media accounts are managed by the Clerk, Assistant Clerk and Deputy Clerk, with access also available to nominated councillors if required.

16.2 Social media must be used responsibly and only for appropriate council purposes when acting in an official capacity.

16.3 Councillors, staff, and authorised users must ensure that their behaviour on social media, when acting as representatives of the council, is respectful and does not bring the council into disrepute. Confidential or sensitive information must not be shared.

16.4 Personal use of social media must not be presented as being on behalf of the council. Users must not give the impression that their personal views are those of the council.

16.5 Any misuse of social media that could damage the reputation of the council may result in appropriate action being taken.

16.6 The use of social media by councillors remains subject to the Members' Code of Conduct.

17 Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.