Radcliffe on Trent Parish Council

Information Technology (IT) Policy and Guidelines

Introduction

The purpose of this IT policy is to set out the parameters on how Radcliffe on Trent Parish Council (the "Council") staff and Councillors should use the technology that is provided in order to perform their roles.

This policy also aims to help raise awareness of the risks associated with using IT and to protect the Council from loss of data.

Council staff are permitted to use Council IT equipment for limited personal use, however as the employer, the Council have the right to monitor or inspect use of any IT equipment provided to a member of staff, where it is reasonable to do so.

It is strongly recommended that staff do not use Council devices for sensitive personal matters, such as online banking or routinely save passwords. In the event employment is terminated, staff are required to immediately surrender any Council owned devices as per their contract of employment. Employees will be given an opportunity to transfer or remove personal information, under the supervision of a designated person, in order to protect Council owned information.

Where an employee is a system administrator, or has superior access controls to a particular system or software, employees will be required to amend access as directed prior to leaving.

IT Resources

This policy is applicable to all Council IT resources, which includes, but is not limited to, host computers, file servers, application servers, mail servers, web servers, workstations, stand-alone computers, laptops, software, data files, mobile phones, removable storage devices, all internal and external computer and communications networks, including the Internet and Cloud services that may be accessed directly or indirectly from the Council's computer network.

Responsibilities

The Senior Proper Officer to the Council, alongside the HR Committee is responsible for the enforcement, monitoring and review of this policy. This policy applies to all staff and

Councillors wherever the location, and any breach or potential breach of this policy and guidelines should be reported immediately to the Senior Proper Officer to the Council, or Chair of the HR Committee.

Privacy Statement

Computers and computer accounts are provided to assist in job performance. Although there should be no expectation of privacy to anything created, stored, sent or received through the Council's computer system or the Internet, files and messages will only be accessed if there is a legitimate business reason to do so. An example of this may be an investigation, whereby the use of Council equipment may assist in matters of process as in order to gather evidence. In such instances, the Council reserves the right to use human or automated means to monitor the use of computer resources at its discretion.

Customer, staff, and other data is subject to the Data Protection Act 2018 (also known as GDPR) and must be treated accordingly.

Website and Social Media

What is published online can make the Council and its staff vulnerable to a range of security threats and or reputational damage. It is also recognised that an online presence may positively benefit the Council, alongside making information easily available.

It is therefore required that no confidential information relating to the Council and its business is published, unless with the expressed permission of the Council. Statutory requirements for publication and information sharing are unaffected by this policy.

Access to the Council's online presence, will be controlled by resolution of the Council to designated staff and or Councillors.

Instances of negligence of Council information, and or inappropriate use of the Councils online presence may result in disciplinary action under the Council's Disciplinary Policy/Code of Conduct.

Artificial Intelligence (AI)

It is acknowledged that AI (such as ChatGPT or CoPilot) can play a supporting role in the operation of business and administration. Where this is utilised, users must ensure documents are checked thoroughly for accuracy and the use of AI should be acknowledged, alongside the author.

Confidential data, such as those relating to HR matters, should not under any circumstances be uploaded to AI applications. Any attempt to do so may result in disciplinary proceedings.

If there is a belief that there is a genuine business reason to do so, or uncertainty exists over the appropriateness of AI, then prior written authorisation from the Senior Proper Officer to the Council is required.

Willful plagiarism of information will be dealt with under the Council's Disciplinary Policy.

Inappropriate or Unlawful Material and/or Use

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate may not be sent by e-mail or any other form of electronic media; or displayed on or stored in any Council system. If you receive any such information, you must inform the Senior Proper Officer of the Council who will then be responsible for taking appropriate action.

The Council's computer resources may not be used for the dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (e.g. viruses or self-replicating code), political material or any other unauthorised use.

Employees must not attempt to discover another User or Administrator password or use any Council computer system to act abusively; attempt to circumvent network security; knowingly run or install programmes intended to damage the computer systems; or deliberately waste computer resources.

Employees must not download or install any unauthorised software onto Council IT equipment. If there is a need, or have identified a potentially beneficial software package, you must in the first instance consult with the Senior Proper Officer of the Council to gain approval before taking any further action. If it is found that unauthorised software has been installed or downloaded without approval, this may be removed and any personal information which this may contain, may not be retrievable.

Employees must not leave a Council or any other IT equipment which may have Council-related business on unattended in a public place. Negligence of Council information and or assets may result in disciplinary action under the Council's Disciplinary Policy.

Copyright and Confidential Material

The Council respects the copyright of those involved in creating and disseminating copyright material, including but not limited to music, films, software, and other literary or artistic material. Employees and Councillors therefore must not make, store, transmit or make available unauthorised copies of any copyright materials on or via any Council system, equipment, or storage media.

If individuals become aware of any misuse of software or violation of copyright law, you must notify the Senior Proper Officer of the Council immediately to enable them to take appropriate action.

Employees must not alter or copy a file belonging to another member of staff without first obtaining permission from the owner of the file or from the Senior Proper Officer of the Council.

Employees must not use the Council's computer systems to snoop or pry into the affairs of other members of staff by unnecessarily reviewing their files or emails.

Any activities or materials that violate these processes are subject to immediate termination and/or removal, under the Council's Disciplinary Policy.

Passwords

To prevent unauthorised access to Council computer resources, a password or PIN must be used. This also applies to all mobile devices that are used to access the Council's data or services.

Individuals are responsible for safeguarding the passwords which are used to access the Council's systems and services.

All passwords, both User and System Administrator passwords, must conform to the following:

1. Passwords should be the minimum length and contain any numbers or special characters as directed by the system being used.
2. Single dictionary words, partner/children/pets' names, dates of birth, common patterns(1234/qwerty) or any information that is publicly available about yourself should not be used.
3. Passwords must be unique to each system. Do not use the same or similar password on other accounts.
4. If there is a need for a password to be written down, for example as a backup for a unique sign-in, this must be placed in a sealed envelope and locked in a drawer, filing cabinet, cupboard or safe.

4. Where 2FA is deployed, you will be required to change your password annually. The exceptions to this are when a System Administrator leaves the business in which case the password will be changed immediately.
5. Passwords must be changed immediately if it is suspected that the password has been compromised in any way and reported to the Senior Proper Officer of the Council.
6. Passwords must not be given to or shared with other people except in an emergency or if agreed in advance by the Senior Proper Officer of the Council. Where a password

is shared in an emergency, the password must then be changed at the first possible opportunity.

7. All default passwords must be changed immediately upon first use.
8. Two factor authentication (2FA) should be used where available.

Following best practice guidance, enforced regular password changes are not required.
As a minimum, systems should lock after 10 unsuccessful login attempts (where technically possible).

The use of https://haveibeenpwned.com/ is recommended to create an alert if your password has been found in a hacking database – at which point you MUST change the password.

Single points of access failures

In order to maintain business continuity, there should be no single point of access failure across any platform, system, interface or software the Council uses.

Whilst maintaining confidentiality and the appropriateness of access rights that are relevant to an individual's role, a minimum of two administrators should always be appointed. This should occur by formal resolution of the Council and may be a mixture of staff and or Councillors. This should be reviewed annually as a minimum, or as required.

Where administrator or approver level access is temporarily reduced to one, for example through absence (planned or unplanned), the existing administrator should appoint a second at the earliest opportunity.

It is acknowledged that in some instances this may need to be done without formal resolution of the Council. In these rare circumstances, authorisation should be sought from the Chair and Vice Chair of the HR Committee. A retrospective approval should take place at the next appropriate meeting of Council.

Administrator access should only be given for a period no longer than necessary, to avoid a single point of access failure, e.g. the second administrator being absent or unavailable. Access should be rescinded as soon as is appropriate to do so and must be reviewed when an individual is no longer in a particular role that requires access e.g. a Councillor is no longer a portfolio holder, or an employee's secondment ends.

In the event of termination of employment or resignation from Council, where an employee/Councillor is a system administrator, or has superior access controls to a particular system or software, the employee/Councillor will be required to amend access as directed prior to leaving.

Clutter Free and Clear Desks

A clutter free approach is promoted to enhance Council's professional image and aid efficiency. To support this, you should:

- Ensure that your surrounding area is kept tidy and bookshelves, pedestal units, etc, should contain only current and relevant information.
- Think before you print. Secure electronic storage is preferred, unless it is absolutely necessary to print documents. Where possible, colour printing should be avoided.
- As they become out of date or superseded, documents, files, etc should be disposed of appropriately and in a timely way.
- Ensure that at the end of the working day, desks are clear with only limited personal items left on show.

At any time when individuals move from their work space, you must ensure that your screen is locked.

At the end of the day, it should be ensured that the PC screen is locked down, any laptops are locked away and monitors are switched off.

General

The Council requires all staff, Councillors, contractors and relevant third-parties to comply with these policies and guidelines. Where applicable, training will be provided in the use of Council systems and to ensure an awareness of security and the requirements to protect Council information.

Staff failing to comply with the above may potentially result in disciplinary proceedings in line with Council's Disciplinary procedures. Councillors may be subject to referral to the Monitoring Officer under the Code of Conduct.

Contractors or relevant third-parties failing to comply may result in the termination of the associated contract.

Date	Item	Next Review
01.12.2012	Document created	2016
24.10.2024	Document revised and updated	19.11.2024
19.11.2024	Full Council consideration and adoption	2026