# Ringshall Parish Council

# IT & Information Management Policy

# V1.0

## Version Control

| | |
|---|---|
| Document Reference | |
| Approval Committee | Full Council |
| Version | 1.0 |
| First Adopted | |
| Next Review Date | May 2020 |

## Policy History

| Version: | Author: | Reason for Issue: | Date: | Approval Minute: |
|---|---|---|---|---|
| 1.0 | Clerk | New Policy | 04/19 | |

## DATA PROTECTION

## 1 ABOUT THIS POLICY

**1.1** This policy outlines the standards Ringshall Parish Council ('the Council') intends to observe in relation to its use of electronic communications of all forms, and its use of IT systems in general.

**1.2** The policy is applicable to all councillors and any employees.

**1.3** The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

## 2 RESPONSIBILITIES

**2.1**

## 3 BREACH OF THIS POLICY

**3.1** Breach of this policy may result in diciplinary action in accordance with the Council's Conduct or Capability procedures and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal. It should also be noted that breach of the policy could also lead to criminal or civil action if illegal material is involved or legislation is contravened. Councillors found to be in breach of this policy may also be deemed to have breached the Code of Conduct and referred to the District Council's Monitoring Officer.

## 4 IT AND COMMUNICATIONS SYSTEMS

**4.1** The Council's IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards users must observe when using these systems and the action the Council will take if users breach these standards.

**4.2** Breach of this policy may be dealt with under the Council's Disciplinary Procedure and, in serious cases, may be treated as gross misconduct.

## 5 EQUIPMENT SECURITY AND PASSWORDS

**5.1** Councillors and officers are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy. Passwords must be set on all IT equipment and passwords must remain confidential and be changed regularly.

**5.2** Users must only log onto Council systems using their own username and password. Users must not use another person's username and password or allow anyone else to log on using their username and password.

## 6 SYSTEMS AND DATA SECURITY

**6.1** Users should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

**6.2** Users must not download or install software from external sources. Downloading unauthorised software may interfere with the Council's systems and may introduce viruses or other malware.

**6.3** Users must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems.

**6.4** Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

**6.5** Users must inform [insert the key contact] immediately if they suspect a computer may have a virus.

## 7 E-MAIL

**7.1** Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

**7.2** It should be noted that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

**7.3** Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

**7.4** For the purposes of council business, users must use a designated email account (or only use the email account provided) in order to receive or send email correspondence.

## 8 USING THE INTERNET

**8.1** Users should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

## 9 PROHIBITED USE OF COUNCIL SYSTEMS

**9.1** Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under the Council's Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

**9.2** Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

**(a)** pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

**(b)** offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or our local community;

**(c)** a false and defamatory statement about any person or organisation;

**(d)** material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

**(e)** confidential information about the Council or any of our staff or our community (except as authorised in the proper performance of your duties);

**(f)** unauthorised software;

**(g)** any other statement which is likely to create any criminal or civil liability; or

**(h)** music or video files or other material in breach of copyright.

## 10 SOCIAL MEDIA

**10.1** This policy is in place to minimise the risks to our Council through use of social media.

**10.2** This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia [, Whisper] [, Instagram] [, Vine] [, Tumblr] and all other social networking sites, internet postings and blogs. It applies to use of social media for Council purposes as well as personal use that may affect our business in any way.

## 11 PROHIBITED USE

**11.1** Users must avoid making any social media communications that could damage the Council's interests or reputation, even indirectly.

**11.2** Users must not use social media to defame or disparage us, Council staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

**11.3** Any misuse of social media should be reported to [council to decide the key contact].

## 12 GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

**12.1** Users should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf.

**12.2** Be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.

**12.3** A data protection breach may result in disciplinary action up to and including dismissal.

**12.4** Members or staff may be required to remove any social media content that the Council believes constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

## 13 BRING YOUR OWN DEVICE (BYOD)

The Council must take appropriate technical and organisational measures against accidental loss or destruction of or damage to personal data. Councillors using their own devices raises a number of data protection concerns due to the fact that these are

owned by the user rather than the data controller. The risks the controller needs to assess are:

- The type of data held.
- Where the data may be stored.
- How the data is transferred.
- Potential data leakage.
- Blurring of personal and business use.
- The device's security capacities.
- What to do if the person who owns the device leaves the Council and
- How to deal with the loss, theft, failure and support of a device.

Councillors and officers using their own devices shall have the following responsibilities:

- Users will not lend their device to anybody.
- Users will inform the Council should they lose, sell, recycle or change their device.
- Users will enable a security pin to access their device and an automatic lock every 5 minutes requiring re-entry of the pin.
- Users will ensure security software is set up on their device and kept up to date.
- Users will not use their device to store Council emails, files and data.