Funtington

Parish Council

Email Policy

Version	1
Name of ratifying body	Funtington Parish Council
Date ratified	6 November 2019
Document manager (Job Title)	Parish Clerk
Date issued	6 November 2019
Review date	October 2021 (unless requirements change)
Electronic location	www.funtingtonpc.org
In the case of hard copies of this policy the content can only be assured to be accurate on the date of issue marked on the document. For assurance that the most up to date policy is being used, staff should refer to the version held on the Funtington website www.funtingtonpc.org	

1. INTRODUCTION

This document describes Funtington Parish Council's policy for email etiquette. It is based on industry best practice and guidance and must be followed by all Funtington Parish Council Staff and Councillors.

2. AIMS AND OBJECTIVES

The objectives of the policy are to ensure that the services made available to Councillors and employees are used:

- In accordance with the values, principles and standards of the Council;

- Ensure GDPR is complied with by ensuring only Funtington Parish Council approved email accounts are used for Council business;

- So as not to incur legal liability; and

- So as not to threaten the integrity of the Council's IT services.

3. SCOPE

This policy applies to all councillors and employees who have access to Council email facilities

4. WHEN TO USE EMAIL

4.1. Email tends to be used for a variety of reasons and can be as informal as arranging refreshments for a meeting to communicating a formal business decision.

4.2. Email is not always the best way to communicate information, as email messages can often be misunderstood and the volume of email messages people receive can be prohibitive to receiving a meaningful reply as a result of email overload.

4.3. All staff that use email have the responsibility of deciding whether email is the most appropriate form of communication. Staff should consider the following factors before sending an email:

4.3.1. **subject:** some subjects are too sensitive to be sent via email, e.g. employee information. Careful consideration needs to be given as it is the responsibility of the sender to decide whether or not email is the most appropriate vehicle for communication in these circumstances;

4.3.2. **speed of transmission:** where information is needed to be communicated urgently and the recipient is expecting it then this is fine. However, if an urgent message needs to be sent and the recipient(s) is/are not expecting anything, then it is probably better to use the phone;

4.3.3. **speed of response:** there is no guarantee that an email will be read as soon as it is sent. If the email requires immediate action then this is probably not the best way to communicate; and

4.3.4. **number of recipients:** do not necessarily use 'reply all' as not everyone in the previous communication necessarily needs to receive the email.

5. WRITING EMAILS

Email is not a secure method of transmission - it should not be assumed that any email communication is secure or private. Users should take this into account particularly when emailing confidential or sensitive information.

5.1. When writing an email, it is important to compose the message with the same care and clarity you would apply to drafting letters and memos, as emails form part of the corporate record under the General Data Protection Regulations and Freedom of Information Act;

5.2. Always ensure that your recipient list is appropriate to avoid causing a nuisance to other colleagues. Is there a need for everyone to see your reply? Also, do you really want everyone to see your reply?

5.3 Be careful about including non-FPC members in the recipient list. It is perfectly acceptable to do so if the non-member is part of a FPC working group or if it is important to include a non-member if you wish to bring the matter to the attention of someone from another agency or organisation e.g. a Member of Parliament;

5.4. Always complete the Subject Line with a clear description of what the email is about, as recipients cannot always distinguish between what they need to look at immediately and what can wait. For example, full council minutes November 2019 for approval;

5.5. Don't be a novelist when composing an email. Ensure language is simple, unambiguous and to the point;

5.6. Avoid using abbreviations and emoticons - don't trade clarity for confusion. Be aware that other colleagues may not know the meaning of informal expressions, such as FWIW (for what it's worth);

5.7. Always, always read email before sending and consider the resultant reaction. Ensuring clarity in the message is time well spent.

5.8. Be polite. Terseness can be misinterpreted. Please and thank you go a long way;

5.9. Never write your email in CAPITAL LETTERS. This implies shouting;

5.10. Never reply in anger. Take a break or sleep on it before responding;

5.11. Don't conduct an argument on email - it is unprofessional.

5.12. Never 'flame' anyone. A flame is an electronic verbal attack. If a flame is received, then please do not respond in anger as this may be regretted later. Users should not engage in exchanging flames and create a 'flamewar';

5.13. Don't mark things as urgent if they aren't, because when you really do have to do an urgent message it may not be treated in the way it deserves;

5.14. Be patient. Not everyone can respond immediately or necessarily have the confidence to communicate using email; and

5.15. Remember: emails sent externally represent and reflect upon the Council.

6. SECURITY

6.1 Access to Councillors' email accounts is restricted to individual users and MUST not be shared accounts;

6.2. The access of each user is controlled by means of their own password;

6.3. Passwords must be kept confidential and not disclosed to others; disclosure could result in email misuse being attributed to the owner of the password;

6.4. Care should be taken not to leave a device that is connected to Councillor emails unattended or unlocked;

6.5. Breaches of security of the computer system e.g. disclosure of personal passwords, giving unauthorised access to emails to external parties, may result in action from the Information Commissioners Office (ICO);

6.6. If you suspect there has been data breach or your email/IT has been hacked you must inform the Parish Clerk immediately. The Parish Clerk will then decide the most appropriate way to deal with the breach; and

6.7. Time should be set aside on a regular basis for "housekeeping", in order to delete old or unwanted items from mailboxes. This is essential in order to ensure the efficient operation of email systems, helps to keep mailboxes organised and ensure compliance with the Council's Document Retention Policy.

7. Breach of Policy and Standards

Any member who knowingly or recklessly contravenes any instruction contained in, or following from, this policy may, depending on the circumstances of the case, have disciplinary action, which could include dismissal from office, taken against them.