GILLINGHAM TOWN COUNCIL

The Town Hall, School Road, Gillingham, Dorset SP8 4QR

Email, Internet and Computer System Use Policy and Procedure for Councillors

Introduction

Gillingham Town Councillors are provided with Councillor email accounts to carry out Town Council business.

This policy relates to Town Councillors' use of email and more general computer use in compliance with the UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018).

All Councillors are required to read this policy at the time of joining Gillingham Town Council.

Objectives

The objectives of the policy are to ensure that the systems made available to Councillors are used:

- In accordance with the values, principles and standards of the Council.
- In compliance with the UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA 2018).
- In a manner that does not threaten the integrity of the Council's IT services.

System Security

Access to the Town Council's IT systems is restricted to Councillors.

- Passwords must be kept confidential and not disclosed to others, as disclosure could result in internet or email misuse being attributed to the owner of the password. All files containing personal data must be password protected.

- Care should be taken not to leave a device that is connected to the internet/ system unattended or unlocked.

- Confidential or personal data and information must not be downloaded to any storage device, eg memory stick.

- Personal data from any contacts databases must not be given to external parties.

- Security breaches, eg disclosure of personal passwords or giving unauthorised access to emails to external parties, may result in action from the Information Commissioners Office (ICO).

- If you suspect there has been data breach or you have been hacked you must inform the Town Clerk immediately. The Town Clerk will act in accordance with the Town Council's Data Breach Policy.

General Email Usage

It is not permitted to use the Gillingham Town Council email for personal purposes. The email provider filters incoming email for porn and spam.

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.

Users should be aware that once an email is sent to an individual outside of the Council, it is beyond the Council's control and is not guaranteed to be confidential.

Continuous virus checking of all incoming email will take place. However, it is possible that a new virus may not be detected so users should be wary of opening attachments to emails from an unknown source – in particular, names ending in "exe" should not be opened. If you receive notification of a virus via chain email do not forward to anyone and contact Dorset Council IT Department.

Hoax and/or suspect emails should be reported to Dorset Council IT Department. They must not be opened or forwarded but "double deleted" ie deleted from the user's Inbox and from the "Deleted Items" folder.

The following email activities may breach the Town Council's Code of Conduct and/or lead to action by the ICO:

- Examining, changing or using another person's files, output or username without explicit authorisation.

- Sending or forwarding any material that is obscene, defamatory or hateful, or which is intended to annoy, harass or intimidate others.

- Sending or forwarding emails which could damage the reputation of the Town Council.

- Soliciting emails that are unrelated to Town Council activities or soliciting non-Council business for personal gain or profit.

- Intentionally interfering with the normal operation of the Town Council's network, including the propagation of computer viruses and the generation of sustained high-volume network traffic.

- Sending or forwarding attachments of such size or arrangement as to cause disruption to the Council's network.

Email Best Practice

- Ensure that each email has a specific target audience.

- Be selective, especially when deciding who should be copied in on an email. This ensures that only those who really require the information receive it and avoids wasteful emails and wasted time/resources.

- If you are copying in recipients who have not given you permission for their email to be circulated, blind copies (Bcc) must be used to protect their details.

- Try to avoid sending large attachments to a large group of recipients as it can significantly increase the load on email servers.

- Time should be set aside on a regular basis for “housekeeping”. Deleting old or unwanted items ensures the efficient operation of the email system, keeps inboxes organised and ensures compliance with the Town Council’s retention policy.

Email Etiquette

Email is all about communication with other people and, as such, some basic courtesy should be observed:

- Always include a subject line in the message.

- When replying to an email, include enough of the original message to provide a context.

- An email signature is a good way of providing detail of who is sending the email and further contact details.

- Consider the tone and language used and the use of plain English, remembering that emails represent and reflect upon the Town Council.

- Avoid using capital letters as this is equivalent to shouting.

Review

This policy was presented to the Finance and Policy Committee on 20 November 2023 for approval, minute no. 614c and ratified at Full Council on 27 November 2023. Future reviews will be carried out annually.

Signed: **Date:**

Mayor of Gillingham