BIGGLESWADE TOWN COUNCIL

Email Policy

This document will be distributed to:

Name

Job Title

Email Address

All Staff

Contents

1. Policy Statement

Biggleswade Town Council will ensure all users of Council email facilities are aware of the acceptable use of such facilities.

2. Purpose

The objective of this Policy is to direct all users of Council email facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can be clear about what is expected of them and their use of email as a communication and recording tool.

3. Scope

This policy covers all email systems and facilities that are provided by Biggleswade Town Council for the purpose of conducting and supporting official business activity through the Council's network infrastructure and all stand alone and portable computer devices.

This policy is intended for all Biggleswade Town Council Members, Committees, Services, Partners, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of email facilities.

The use of email facilities will be permitted providing staff have received appropriate training (where applicable) and have confirmed by signing the Council's Code of Conduct that they accept and agree to abide by the terms of this policy.

Inappropriate use of email facilities by staff will be regarded as a disciplinary offence.

4. Definition

All email prepared and sent from Biggleswade Town Council email addresses or mailboxes, and any non-work email sent using Biggleswade Town Council ICT facilities is subject to this policy.

5. Risks

Biggleswade Town Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Viruses, malware etc.
- Increased risk of data loss and corresponding fines.
- Inappropriate access to and unacceptable use of the Council's network, software, facilities and documents.
- Inadequate destruction of data.

- The non-reporting of information security incidents.
- Inconsistency in how users deal with ‘secure’ documents.
- The impact of insufficient training for users.
- The sharing of passwords.
- Incorrect or inappropriate classification of documents.
- Risk of reputation damage and further loss in public confidence.
- Operational difficulties providing services.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6. Applying the Policy

6.1. Email as Records

All emails that are used to conduct or support official Biggleswade Town Council business must be sent using a “@biggleswadetowncouncil.gov.uk” address.

Non-work email accounts must not be used to conduct or support official Biggleswade Town Council business.

Members and users must ensure that any emails containing sensitive information must be sent from an official Council email. All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Biggleswade Town Council business should be considered to be an official communication from the Council.

In order to ensure that Biggleswade Town Council is protected adequately from misuse of e-mail, the following controls will be exercised:

All official external e-mail must carry the following disclaimer:

DISCLAIMER
You should be aware that all e-mails received and sent by this Council are subject to the Freedom of Information Act 2000 and therefore may be disclosed to a third party. (The information contained in this message or any of its attachments may be privileged and confidential and intended for the exclusive use of the addressee). The views expressed may not be official policy but the personal views of the originator.

If you are not the addressees any disclosure, reproduction, distribution, other dissemination or use of this communication is strictly prohibited.

If you received this message in error, please return it to the originator and confirm that you have deleted all copies of it.

All messages sent by this organisation are checked for viruses using the latest antivirus products.

This does not guarantee a virus has not been transmitted. Please therefore ensure that you take your own precautions for the detection and eradication of viruses.

Whilst respecting the privacy of authorised users, Biggleswade Town Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act.

Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council's ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the Town Councils Freedom of Information guide.

6.2. Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or **PROTECTED** or **RESTRICTED** information, or of communicating in the particular circumstances.

All emails sent to conduct or support official Biggleswade Town Council business must comply with communications standards.

Members must ensure that any emails containing sensitive information must be sent from an official council email.

Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult their line manager prior to commencing any associated activity or process.

IT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of **PROTECTED** or **RESTRICTED** material concerning the activities of the Council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council into disrepute.

6.3. Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) must not be forwarded using Biggleswade Town Council systems or facilities.

6.4. Mail Box Size

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addresses is discouraged.

Users are provided with a limited mail box size to reduce problems associated with server capacity.

Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox.

6.5. Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded. The monitoring of email (outgoing and incoming) traffic will be undertaken so that Biggleswade Town Council

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.

Monitoring of content will only be undertaken by staff specifically authorised for that purpose These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Determining if communications are relevant to the business.

Where a manager suspects that the email facilities are being abused by a user, they should contact the Town Clerk. Designated staff from the Council's outsourced IT provider can investigate and provide evidence and audit trails of access to systems. The Council will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email is strictly forbidden unless the employee has given their consent, or their email needs to be accessed by their line manager for specific work purposes whilst they are absent. Managers must only open emails which are relevant.

6.6. Categorisation of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate. It is advisable that all emails are protectively marked in accordance with the HMG Security Policy Framework (SPF). The marking classification will determine how the email, and the information contained within it, should be protected and who should be allowed access to it.

The SPF requires information to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependent on this scheme.

The classifications are:

- Unclassified
- PROTECT
- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

Information up to **RESTRICTED** must be marked appropriately using the SPF guidance.

6.7. Security

Emails sent between biggleswadetowncouncil.gov.uk address are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss.

There is a risk that copies of the email are left within the public communications system. Therefore, **PROTECTED** and **RESTRICTED** material must not be sent via email outside a closed network.

6.8. Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure of whether they should pass on information, they should consult the Town Clerk.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained.

Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of Biggleswade Town Council.

Care should be taken when addressing all emails, but particularly where they include **PROTECTED** or **RESTRICTED** information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent **PROTECTED** or **RESTRICTED** material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the Council's outsourced IT provider in the first instance.

6.9. Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Biggleswade Town Council's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to the Council's outsourced IT provider.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities.
- Must not forward virus warnings other than to the Council's outsourced IT provider.
- Must report any suspected files to the Council's outsourced IT provider's helpdesk.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use three functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted.

7. Policy Compliance

If any user is found to have breached this policy, they may be subject to Biggleswade Town Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

8. Policy Governance

The following table identifies who within Biggleswade Town Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible

Town Council and Committees.

Accountable

Town Clerk.

Consulted

Town Councillors and Committee Members.

Informed

All Council Employees, All Temporary Staff, All Contractors.

9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.