Trowbridge Town Council

Working with the Community

E-mail, Internet, Social Media & Computer Use Policy

1. INTRODUCTION

Trowbridge Town Council provides Internet, Wi-Fi and E-mail facilities for use by Councillors, employees and volunteers who have access to a desktop PC, laptop, smartphone, tablet or other computer device. This document sets out the Council's policy for the use of these facilities and services and for general computer use.

2. OBJECTIVES

The objectives of the policy are to ensure that the services made available to users are used:

- In accordance with the values, principles and standards of the Council.
- Appropriately, in terms of Council time and resources consumed.
- So as not to incur legal liability.
- So as not to threaten the integrity of the Council's IT services.

3. ACCEPTANCE OF THE POLICY

The policy applies to all Council employees and also to Councillors where they utilise Council systems and facilities. For the purpose of this document the definition of "employee" is:- *'any individual who is paid by, or works as a volunteer for, the Town Council including full time, part time, temporary or casual work.'*

All employees are required to sign to indicate their acceptance of the policy at the time of joining the Council and will be asked to re-affirm their understanding and acceptance of the policy when changes are made. Each employee is responsible for individually complying with this policy. Managers should oversee and supervise use within their areas.

4. SECURITY

Access to the Council's computer network through its servers is restricted to individual users who have been given access rights by the Facilities Manager

- Access for each user is controlled by means of a password.
- Passwords must be kept confidential and not disclosed to others; disclosure could result in Internet or E-mail misuse being attributed to the owner of the password.
- Care should be taken not to leave a computer device that is connected to the Internet/network unattended or unlocked.
- Under no circumstances should anyone outside of the Council be given access to the Council's computer based services/main drives without first obtaining permission from the Administrator (currently the Facilities Manager). A visitor account can be made available for agreed users.
- Breaches of security of the computer systems e.g. disclosure of personal passwords thus giving unauthorised access to the system, may result in disciplinary action which could result in dismissal.
- Public using the Council's services (i.e. those who hire the venue) can have access to Internet services provided via WIFI and using the 'Civic Centre' SSID only.

5. GUIDANCE

This section of the document provides guidance on the acceptable use of the Council's E-mail and Internet services and electronic databases.

5.1 E-mail Usage

The Council's E-mail system enables users to E-mail other employees, councillors and external individuals and organisations. Users should be aware that once an e-mail is sent outside the Council, it is beyond the Council's control and is not guaranteed to be confidential.

5.1.2 **Prohibited E-mail Activities**

The following E-mail activities may result in disciplinary action, up to, and including, dismissal:

- Examining, changing or using another person's files, output or user name 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 E-mails which are likely to damage the reputation of the Council.
- Sending or forwarding electronic chain letters.
- Soliciting E-mails that are unrelated to Council activities or soliciting non-Council business for personal gain or profit.
- Intentionally interfering with the normal operation of the Council's network, including the propagation of computer viruses and the generation of sustained high volume network traffic.
- Your work email address should not be linked to any personal social media profile or billing/account service (ITunes, PayPal etc.).
- Sending or forwarding attachments of such size or arrangement as to cause disruption to the Council's network *(see Section 5.1.5)*.

5.1.3 **Acceptable Personal E-mail Use**

The limited use of E-mail for personal purposes is permitted, subject to the following:

- Personal use of E-mail facilities is permitted outside of normal working time and should not interfere with the performance of duties.
- Personal use should not cause any damage to computers or networks, or any difficulty or distress to others.
- The use does not breach any of the items shown in the Prohibited E-mail Activities *(see 5.1.2 above)*.

Employees who use the Council's E-mail facility for personal use expressly consent to the conditions detailed in this document. Employees who do not accept the conditions under which the Council's E-mail facilities can be used for personal purposes must not use the facility.

5.1.4 **E-mail Awareness**

E-mail is not a secure method of transmission – it should not be assumed that any
E-mail communication is secure or private while in transit between our server and the recipient's server. Users should take this into account particularly when E-mailing confidential or sensitive information.

5.1.5 **E-mail Best Practice**

Users should:

- Ensure that each E-mail has a specific target audience.
- Be selective, especially when deciding who should be copied in on an E-mail. This ensures that only those who really require the information receive it, and avoids wasteful E-mails and wasted time/resources.
- The circulation of E-mails with attachments to large groups should be avoided. Attachments are copied to every user; therefore an E-mail with an attachment sent to all staff will be copied over 40 times, taking up substantial storage space.
- Information for the attention of several users should be saved to the shared drive and an E-mail sent to notify readers of its location.

- Users should not send attachments internally which are over 4mb in size, nor should they send external E-mails with large attachments. External E-mails should be limited to no more than 10mb in size. For files larger than 10mb use

- www.wetransfer.com. For assistance with checking the size of E-mails and attachments, please contact the Administrator.
- When sending E-mails to a large number of people the recipients' addresses should be entered into the **Bcc** (blind copy) field. Users should contact the Administrator if assistance is required.
- E-mails should not be kept in separate folders in an individual's folder list longer than is necessary, if at all. Attachments and/or important E-mails should be saved in the relevant folders/files on the main system.
- 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 the E-mail system and helps to keep mailboxes organised. The 'Inbox', 'Sent Items' and 'Deleted Items' folders should be examined as part of a housekeeping routine, performed at a minimum frequency of once a month. Contact the Administrator for assistance.
- The Council's E-mail system should not be used to circulate non-Council related information such as items for sale, personal social events and news items. A notice board facility is provided where such items can be posted and read by staff and Members.

5.1.6 E-mail Etiquette

E-mail is all about communication with other people, and as such some basic courtesy should be observed.

- Always include a subject line in your message.
- When replying to an E-mail, include enough of the original message to provide a context.
- An E-mail signature is a good way of providing detail of who is sending the E-mail and the details of how to respond. Any advertising of Council events done via the signature facility must be kept up to date.
- Consider the tone and language used, and the use of plain English. When sent externally E-mails represent and reflect upon the Council.
- Avoid using capitals throughout as this is equivalent to shouting.

5.2 Internet Usage

Use of the Internet by Council employees is permitted and encouraged where such use is relevant to, and in pursuit of, the work of the Council. Internet use is regarded as an aid to the normal responsibilities of the employee; it should be used in a manner that is consistent with the Council's standards of proper conduct, courtesy and customer care. Basic training will be provided for all Internet users as well as guidance on Internet etiquette. More advanced training will be provided where necessary through the Administrator.

5.2.1 Prohibited Internet Activities

The following practices are considered unacceptable and may result in disciplinary action being taken. The Council also reserves the right to report any illegal activity to the appropriate authorities.

- Visiting Internet sites that contain pornographic, obscene or otherwise objectionable material.
- Using the Internet for gambling or illegal activities.
- Accessing social networking sites for non-Council related activities e.g. Facebook, other than at permitted times (*see 5.2.2*).

- Making or posting indecent, offensive or discriminatory remarks, proposals or materials.
- Uploading, downloading or otherwise transmitting commercial software or copyright material in violation of its copyright.
- Revealing or publicising confidential information including financial information, personal information, the information in the Council's confidential files and network access information.
- Other inappropriate uses that may be identified and publicised by the Administrator.

5.2.2 **Acceptable Personal Internet Use**

The Internet is provided for Council use. The Council recognises that many employees use the Internet for personal purposes and that many employees participate in social networking on websites such as Facebook and Twitter. The use of the Internet including social networking websites for personal use or research is permitted subject to the following:

- The use takes place during lunch hours or outside of normal working time.
- The amount of time spent on personal use does not impact on work duties or reduce resources for others.
- The use does not breach any of the items shown in the Prohibited Internet Activities, *(see 5.2.1 above).*

Employees who use the Council's Internet facility expressly consent to the conditions detailed in this policy. Employees who do not accept the conditions under which the Council's Internet facilities can be used for personal purposes must not use the facility.

5.2.3 **Social Media**

The Council respects an employee's right to a private life. However, the Council must also ensure that confidentiality and its reputation are protected. It therefore requires employees using social networking websites to:

- be cautious when they can be identified as working for the Council;
- ensure that they do not conduct themselves in a way that is detrimental to the Council; and
- take care not to allow their interaction on these websites to damage working relationships between members of staff, Councillors, customers and members of the public.

5.2.4 **Security and identity theft**

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private. Employees should never send abusive or defamatory messages. Employees must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees should:

- ensure that no information is made available that could provide a person with unauthorised access to the Council and/or any confidential information; and
- refrain from recording any confidential information regarding the Council on any social networking website.

5.3 Database Usage

In accordance with the Data Protection Act, no personal details/data from any contacts databases e.g. TTC Contacts, should be given out to external parties at any time. No personal data/databases should be kept on any storage facility e.g. CDs, DVDs, 3¼" discs, USBs, laptops

or personal home based computers, as this could result in legal action from third parties. Breaches of the above may result in disciplinary action being taken.

6. ACCESS CONTROL AND MONITORING

The 'Regulation of Investigatory Powers Act 2000' authorises monitoring for a number of purposes. The Council has selected the least intrusive methods of monitoring. While the Council has no wish to interfere with the privacy of its workers, it is required to discharge a number of legal duties that are laid down on all employers and managers of computer systems concerning what passes through, and is stored within, their systems – for example, to ensure that these are not used for criminal or other improper purposes, to prevent the spread of computer viruses, and to avoid other situations that might corrupt or degrade the operations of the Council's computer systems or those of other systems elsewhere. Thus, the Council reserves the right to monitor Internet use, access email and other material on its computer systems from time to time for various reasonable and necessary purposes. The Council also reserves the right to retain information that it has gathered on employee's use of the computer systems for a period of one year. The council also reserves the right to use any information it has retained through monitoring and control , if deemed necessary, as evidence in any disciplinary issues.

Such monitoring will be kept to a reasonable minimum and every care will be taken to comply with all applicable data protection and privacy legislation in respect of the confidentiality of any material that is monitored insofar as this does not conflict with duties laid down in other legislation or with the prevention of harassment or other serious breaches of the Council's disciplinary code.

- Personal Emails will not be read by anyone except the sender or recipient if they are clearly marked as such. However, this will not be the case where access to the content of the Email is required for the prevention or detection of a suspected crime or to prevent the inappropriate use of Email as detailed below.
- Any investigation other than day-to-day monitoring requires the written authority of the Town Clerk or his/her nominee in order to take place.

6.1 Methods of Monitoring

Sonic Wall or WatchGuard monitors the access to websites according to their Internet Point (IP) address. This is a security device installed to the Council's system which is controlled and reviewed by the administrators

6.1.1 Blocking

The Council makes use of blocking facilities to provide first line protection against unsuitable sites.

6.2 Monitoring of Internet Usage

The Council reserves the right to monitor Internet usage, but will endeavour to inform employees when this is to happen and the reasons for it. The Council considers that valid reasons for checking Internet usage include suspicions that the employee has:

- been spending an excessive amount of time viewing websites that are non-Council related; or
- acted in a way that damages the reputation of the Council and/or breaches commercial confidentiality.

6.3 E-mail Monitoring

The Council monitors E-mail activity, so that compliance with this policy and other relevant policies and regulations can be effectively managed.

6.4 E-mail Viruses and Hoaxes

Continuous virus checking of all incoming E-mails will take place. However, it is possible that a new virus may not be detected by the Council's virus scanner and users should be wary of opening attachments to E-mails from an unknown source; in particular attachments with names

ending in ".exe" should not be opened. If you receive notification of a virus via chain E-mail do not forward to anyone. Advise the Administrator of the details. They will investigate the virus threat. Hoax and/or suspect E-mails should be reported to the Administrator. They should not be opened or forwarded but "double deleted" i.e. deleted from the user "Inbox" and then also deleted from the "Deleted Items".

6.5 E-mail Filtering

Users should note that the Council's Internet Service Provider filters incoming E-mail for porn and spam as well as scanning for E-mail viruses.

6.6 Software

No unauthorised software is to be run or installed on Council computers either via downloads from the Internet or by disks, CDs or flash drives. All disks, CDs and flash drives must be virus checked by the Administrator before use.

6.7 Disciplinary action

If the Council monitors employees' Internet use to ensure that it is in accordance with this policy, access to the Internet may be withdrawn in any case of misuse of this facility. If appropriate, disciplinary action may also be taken in line with the Council's disciplinary policy. An employee who makes a defamatory statement that is published on the Internet may be legally liable for any damage to the reputation of the individual concerned. An employer may be vicariously liable for the acts of an employee done in the course of employment, even if performed without the consent or approval of the employer. A company can sue if a defamatory statement is made in connection with its business or trading reputation.

7. SYSTEM USE

This section sets out the correct use of the Council's computer system

7.1 Correct Use of Drives

7.1.1 Device C:\ and Personal U:\ drives

- Every user is provided with a personal U:\ drive which should be used to store personal data they wish to keep i.e. appraisals or diaries. It is not to be used for storing personal pictures or for work which should be on the Public P:\ drive where it is shared by others.
- The PC's C:\ drive can be used to store documents where you can work from them quicker than working from the P:\ drive. You should save the document back onto the P:\ Drive at the end of the day to ensure it is backed up. Any documents saved locally to the C:\ drive are not secure from other users of that device and will not be backed up. If the PC becomes faulty it is very likely you will not be able to retrieve the document again.

7.1.2 Shared and Public P:\, R:\, S:\, and T:\ drives

- All documents/files are to be stored in the correct folders on the computer system.
- Any separate personal folders holding Council documents are unnecessary and will be deleted.
- Users found to be persistently abusing this policy may face disciplinary action.

7.1.3 Housekeeping of all drives

- Any photographs taken by staff or professional bodies should remain on a disc and filed for general access when required. A small selection of photos can be uploaded to the Public drive which can be used for advertising purposes. Multiple photographs of the same thing must be reduced to one copy to save storage and back-up costs.

8. Employers and use of the Internet

At no stage during the recruitment process will the Council conduct searches on prospective employees on social networking websites. Throughout the recruitment process, all job applicants are protected from discrimination on the grounds of sex, marital status, race, disability, age, sexual orientation and religion or belief.

- As social networking websites display personal details such as age, religion and beliefs and sexual orientation, employers should avoid using these websites to look for background information about job applicants. If an employee is subjected to harassment on grounds of sex, marital status, race, disability, sexual orientation, religion or belief or age, he or she may have grounds to bring a complaint to an employment tribunal under the relevant anti-discrimination legislation. Employers should be aware that harassment can take place in online environments such as social networking websites. Employers can be liable for anything done by an employee in the course of his or her employment, whether or not it was done with the employer's knowledge or approval. An employer can defend itself by taking reasonably practicable steps to prevent the harassment.
- Under common law, there is an implied duty of trust and confidence between an employer and an employee. Employees who have access to confidential information should be made aware of the consequences of misuse and that even inadvertent disclosure could result in disciplinary action.

Notes

- An employer can monitor Internet use to detect unauthorised or excessive use, but should circulate notices explaining what constitutes authorised use and what does not. Issuing a policy and circulating it to all employees will satisfy the requirement for an employer to inform employees that it is monitoring Internet use.
- Employers must take positive action to eliminate employee behaviour that could cause distress and anxiety to others in the workplace, including activity taking place on social networking websites.
- Employers are advised to enforce a zero-tolerance policy in relation to bullying and harassment. Employers should outline clearly what is regarded as unacceptable use of the Internet at work.
- Employers should also consider making it clear to employees that any inappropriate social use of the Internet outside the workplace could also result in disciplinary action if it brings the employer's reputation into disrepute or exposes it to potential liabilities.

Warning

An employer may be in breach of the Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 if an employee is not told that monitoring of the Internet will occur.

Lance Allan – Town Clerk & Proper Officer

Signed . . . . . Dated . . . . . .

Approved at the meeting of the Policy & Resources Committee on 3rd November 2015.
Amendments will be made as and when the size and nature of the Council changes or when new legislation is introduced. Otherwise date of next review November 2019.

TROWBRIDGE TOWN COUNCIL

E-mail, Internet, Social Media and Computer Use Policy

ACCEPTANCE SLIP

I have received, read and understood the Council's E-mail, Internet, Social Media and Computer Use Policy. I understand that:-

- My use of E-mail and the Internet may be monitored for management and security purposes.
- Breaches of the policy may result in disciplinary action being taken against me.

Signed ……...

Name ……...

Date ……...

Please return completed forms to Juliet Weimar, HR Manager