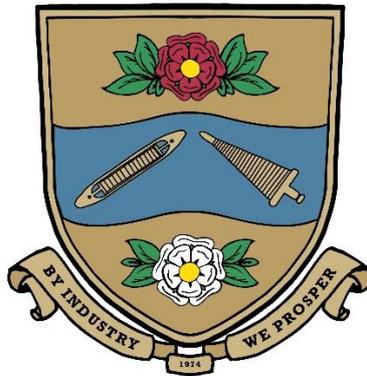


# Todmorden Town Council



TODMORDEN TOWN COUNCIL

# Information Technology Policy

## Computer Equipment, Network, Internet and Email

Prepared by Colin Hill Town Clerk

Date: July 2020

Next Review date: May 2022

Adopted at Emergency Committee 29th July 2020

## **CONTENTS**

- 1. Introduction**
- 2. Objectives**
- 3. Virus Protection Procedures**
- 4. Use of Computer Equipment – Employees**
- 5. Use of Computer Equipment – Employees**
- 6. Use of Printers**
- 7. E- MAIL**
- 8. E- MAIL Procedures – Authorised Use**
- 9. E- MAIL Reporting and Sanction**
- 10. Internet**
- 11. Internet Procedures Acceptable/ Unacceptable Use**
- 12. Monitoring- Employees**
- 13. Use of Social Networking Sites**
- 14. Intellectual Property Rights**
- 15. Network Security**

## **1 Introduction**

- 1.1. The purpose of the Computer Equipment, Internet and E-mail policy is to provide a framework to ensure that there is continuity of procedures in the usage of equipment internet and e-mail within the Council.
- 1.2. The internet and e-mail system are important communications facility within the Council and provide us with contact with internal and external sources necessary for us to carry out our day to work requirements.
- 1.3. To ensure that we can utilise the system to its optimum, this policy provides maximum use of the facility, whilst ensuring compliance with legislation.
- 1.4. This Policy applies to
  - a) Employees and Councillors where Computers have been provided by the Town Council
  - b) Employees and Councillors where Printers have been provided by the Town Council
- 1.5. Where Councillors use their own devices to access their own Town Council Email address, there is an expectation that their devices and or internet connection will provide a measure of virus protection.
- 1.6. Councillors receive Council equipment based on a loan and the equipment at all times remains the property of Todmorden Town Council.
- 1.7. Any individual Councillor on leaving the office of Town Councillor, undertakes to return such equipment to the Town Clerk

## **2 Objectives**

- 2.1 To protect Councillors, Employees and the Employer from dangers that arise through Internet usage e.g. virus attacks, trojans, spy technology.
- 2.2 To ensure that all Employees and Councillors make every effort to protect both hardware and software, where issued by the Council, from misuse and or damage.
- 2.3 To collectively minimise the potential for serious disruption to Town Council business through the introduction of a virus that could disable operations.

## **3 Virus Protection Procedures**

- 3.1 In order to prevent the introduction of virus contamination into the software System the following must be observed when using Council provided equipment

- a) unauthorised software including public domain software, USBs, external hard drives, CDs or internet downloads must not be used
- b) all software must be virus checked using standard testing procedures before being used – this is provided by the Town Council on Town Council issued Laptops

#### **4 Use of Computer Equipment - Employees**

4.1 To control use of the Town Council's computer equipment and reduce the risk of contamination the following will apply for employees:-

- only authorised staff should have access to the computer equipment.
- only authorised software may be used on any of the computer equipment.
- only software that is used for business applications may be used.
- no software may be brought onto or taken from the Town Council's premises without prior authorisation;
- unauthorised access to the computer facility will result in disciplinary action; and
- unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

#### **5 Use of Computer Equipment – Where Issued to Councillors**

5.1 To control use of the Town Council's computer equipment and reduce the risk of contamination the following will apply for Councillors

- only the Councillor provided with a laptop should have access to the computer equipment.
- only software authorised by the Town Clerk may be used on any of the computer equipment.
- only software that is used for business applications may be used.
- no software may be brought onto or taken from the Town Council premises without prior authorisation.
- unauthorised access to the computer facility and or unauthorised copying and/or removal of computer equipment/software will result in a charge of misconduct being brought.

#### **6 Use of Printers – Where Issued to Town Councillors and Employees for Home Working**

6.1 Where printers are provided by the Town Council to Councillors and Employees, there is an expectation that these will predominantly be used for Town Council business, but personal use is allowed.

6.2 Replenishment Print Cartridges will be provided by the Town Council but where the extent of replenishment is more frequent than may be regarded as

normal, a financial contribution may be sought.

- 6.3 Replenishment Paper will be provided to enable Town Council related items to be printed, but where the extent of replenishment is more frequent than may be regarded as normal, a financial contribution may be sought.
- 6.4 Any printers not working should be reported to the Administrative Officer, who will arrange for a service visit to be carried out

## **7 E-MAIL**

- 7.1 The use of the e-mail system is encouraged. Used correctly it is a facility that is of assistance to both Employees and Councillors
- 7.2 Inappropriate use however causes many problems including distractions, time wasting and legal claims. The procedure sets out the Town Council's position on the correct use of the e-mail system.
- 7.3 All Councillors will be provided with a Council e-mail address and should use this for all council business
- 7.4 Employees and Councillors are reminded that any e-mail sent or received in their capacity as an Employee or Town Councillor is Council data and any e-mails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act

## **8 E-MAIL Procedures - Authorised Use**

- 8.1 The e-mail system is available for communication and matters directly concerned with the legitimate business of the Town Council. Employees and Councillors using the e-mail system should give particular attention to the following points:
  - a) all comply with any internal communication standards.
  - b) use appropriate language to avoid unintentional misunderstandings
  - c) e-mail messages and copies should only be sent to those for whom they are particularly relevant.
  - d) check with the sender if there is any doubt regarding the authenticity of a message.
  - e) e-mail should not be used as a substitute for face-to-face communication or telephone or virtual contact. Abusive e-mails must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding.
  - f) if e-mail is confidential, the user must ensure that the necessary steps are taken to protect confidentiality. The Town Council will be liable for infringing copyright or any defamatory information that is circulated either within the Town Council or to external users of the system; and respect the confidentiality of information contained within emails, even if

encountered inadvertently.

- g) do not open any attachment unless certain of the authenticity of the sender
- h) offers or contracts transmitted by e-mail are as legally binding on the Town Council as those sent on paper.
- i) emails which create obligations or give instructions on behalf of the Council must be sent by officers only, not Councillors

8.2 The Town Council will not accept the use of the e-mail system for unofficial or inappropriate purposes, including:

- a) any messages that could constitute bullying, harassment or other detriment.
- b) personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
- c) on-line gambling.
- d) accessing or transmitting pornography.
- e) transmitting copyright information and/or any software available to the user; or
- f) posting confidential information about other employees, the Company or its clients or suppliers.

## **9 E-MAIL Reporting and Sanctions**

9.1 If a Councillor receives an email from a staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Town Clerk or if the email was from the Town Clerk, to the Chair of the Staffing Committee, who will consider use of the Council's formal disciplinary procedure.

9.2 If a staff member receives an email from another staff member which they believe is contrary to the guidance provided in this policy, it should be reported to Town Clerk, or if from the Town Clerk, to the Chair of Staffing Committee who will consider use of the Council's formal disciplinary procedure.

9.3 If a staff member receives an email from a Councillor which they believe is contrary to the guidance provided in this policy, the staff member is entitled to consider use of the Council's grievance policy and/or report the issue through the procedures outlined in the Member's Code of Conduct

## **10 Internet**

10.1 Where appropriate, duly authorised staff and or Councillors are encouraged to make use of the Internet as part of their official and professional activities.

10.2 Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the Town

Council's name.

- 10.3 Where personal views are expressed, a disclaimer stating that this is the case should be clearly added to all correspondence.
- 10.4 The intellectual property right and copyright must not be compromised when publishing on the Internet.
- 10.5 The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal, or in the case of a Councillor a charge of misconduct.

## **11 Internet Procedures – Acceptable/Unacceptable Use**

- 11.1 The internet system is available for legitimate business use and matters concerned directly with the job being done. Employees and Councillors using the internet system should give attention to the following points:
- a) comply with all internet standards.
  - b) access should be for business use only where Employees and Councillors are using Town Council provided equipment
- 11.2 The Town Council does not expect any use of the Internet system for unofficial or inappropriate purposes, including:
- a) accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights.
  - b) non-compliance of our social networking policy.
  - c) connecting, posting or downloading any information unrelated to their employment and in particular pornographic or other offensive material.
  - d) engaging in computer hacking and other related activities or attempting to disable or compromise security of information contained on the Town Council's computers.
  - e) sending or posting of discriminatory, harassing, threatening messages or images.
  - f) obtaining, using, or disclosing another staff member's password without authorisation
  - g) using computers to perpetrate any form of fraud, and/or software, film, or music piracy
  - h) sharing confidential material or proprietary information outside of the Council
  - i) sending or posting information that is defamatory to the Council, its services, Councillors and/or members of the public
  - j) sending or posting chain letters, solicitations or advertisements not related to Council business or activities

- k) passing off personal views as those representing the Council  
**Activities (c and d) may constitute a criminal offence.**

11.3 If a staff member is unsure about what constitutes acceptable internet usage, then he/she should ask his/her line manager for further clarification.

## **12 Monitoring – Employees**

12.1 The Town Council reserves the right to monitor all e-mail/internet activity by Employees for the purposes of ensuring compliance with Town Council policies and procedures and of ensuring compliance with the relevant regulatory requirements.

- a. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.
- b. Monitoring your usage will mean processing your personal data. You may read more about the data we hold on you, why we hold it and the lawful basis that applies in the Employee privacy notice.
- c. Under no circumstances will any information that is discovered be disclosed to a third party and all investigations will strictly adhere to the Data Protection Act 2018
- D. Any information obtained from monitoring will be considered by the Council which reserves the right to determine what is and is not suitable.

## **13 Use of Social Networking Sites**

13.1 Any work-related issue or material that could identify an individual who is a client or work colleague, and/or which could adversely affect the Town Council, a client or our relationship with any client must not be placed on a social networking site.

13.2 This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment or mobile device, unless as part of the Council's normal promotional, messaging and provision of information use as approved by the Town Clerk.

13.3 Employees must not use the Internet for personal use, e.g. visiting social networking sites including Facebook and Twitter during normal working hours unless it is during their break time.

## **14 Intellectual Property Rights**

- 14.1 All intellectual property rights in all work created by Employees in the course of performing any services for the Council or in any way related to the services provided to the Council shall belong solely to the Council (Service IPR).
- 14.2 This includes but is not limited to all copyright, design rights, trademarks, patents, rights in data and all other equivalent rights whether or not registered or capable of registration, including the right to apply for any of the foregoing.
- 14.3 Employees hereby irrevocably and unconditionally waive in favour of the Town Council all moral rights attached to any Service IPR.
- 14.4 Employees will, at the Council's request, sign such documents and carry out all such acts as the council may require to fully and effectively vest in the Council, free from encumbrances, all rights, title and interest in the Service IPR, so that the council may obtain patents, registered designs or other protection in its own name in the united kingdom and/or other countries.

## **15 Network Security**

- 15.1 Any problems with network security should be immediately referred to the IT provider by the Administrative Officer.
- 15.2 Problems with personal computers should only be referred to the IT provider after reporting to the Administrative Officer
- 15.3 Employees should not attempt to resolve the problem themselves unless they are absolutely sure of their capability to do so.
- 15.4 Remote access to the Town Council network is permitted for Employee use when working from home
- 15.5 Passwords will be changed on an annual basis unless compromised at any Time, at which stage, they will be changed immediately.