

# Thame Town Council

## IT Policy

### 1. Objective

- 1.1 To protect both employees and employers alike from the many dangers that arise through Internet usage, e.g. virus attacks, Trojans, spy technology.
- 1.2 To ensure that all employees operate their computers in accordance with the Data Protection Act 1998 and make every effort to protect both hardware and software from misuse and/or damage.
- 1.3 To prevent employees from sending, soliciting or downloading inappropriate material from the Internet or email technology.

### 2. Use of Computer Equipment

- 2.1 In order to control the use of the Council's computer equipment and reduce the risk of contamination the following will apply.
- 2.2 The introduction of new software must be authorised by the Town Clerk.
- 2.3 Only authorised staff should have access to the Council's computer equipment. Unauthorised access to the computer facility will result in disciplinary action. Employees are personally responsible at all times for the protection of Council data and information including printed materials.
- 2.4 No software may be brought onto or taken from the Council's premises without prior authorisation. Unauthorised copying and/or removal of computer equipment/software or downloading information onto memory sticks will result in disciplinary action. ~~Such actions could lead to dismissal~~
- 2.5 Employees are responsible for their own workstations and keyboards which must be kept clean. In addition every effort should be taken to protect them from hazards, e.g. cups of tea or coffee which have the potential to spill onto keyboards.
- 2.6 Passwords will be updated annually. The computer will prompt this change with a pop-up asking you to change the password.

### 3. Confidentiality

- 3.1 Employees should not reveal confidential data to any third party. This includes personal or sensitive data (as defined under Data Protection Act 1998), computer software source codes, login details and passwords.
- 3.2 Should there ever be a reason to provide such information it must be with the permission of Town Clerk and only in accordance with Data Protection Guidelines.

### 4. Email

- 4.1 The Email system is available for communication and matters directly concerned with the

legitimate business of the Council. Employees using the Email system should give particular attention to the following points:

- i All comply with Council communication standards
  - ii Email messages and copies should only be sent to those for whom they are particularly relevant and all documents sent must be as PDF's
  - iii Email should not be used as a substitute for face-to-face communication or telephone contact. Flame mails (i.e. Emails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding
  - iv If email is confidential, the user must ensure that the necessary steps are taken to protect confidentiality.
  - v The Council will be liable for infringing copyright or any defamatory information that is circulated either within the Council or to external users of the system
  - vi Offers or contracts transmitted by Email are as legally binding on the Council as those sent on paper
- 4.2 The Council will not tolerate the use of the Email system for unofficial or inappropriate purposes, and if caught an employee may face disciplinary action. This includes:
- i. Any messages that could constitute bullying, harassment or other detriment;
  - ii. Personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
  - iii. On-line gambling
  - iv. Accessing or transmitting pornography
  - v. Transmitting copyright information and/or any software available to the user; or
  - vi. Posting confidential information about other employees, the Council or the public or suppliers
- 4.3 Unauthorised or inappropriate use of the Email system may result in disciplinary action, which could lead to dismissal.
- 4.4 Email inboxes should be cleared out on a regular basis and no inboxes should reach the maximum folder size as set by the Town Council.
- 4.5 **The Council operates an open policy in regard to access to employees' emails and the Town Clerk reserves the right to automatic permissions.**

## **5. Internet**

- 5.1 Where appropriate, staff are encouraged to make use of the Internet as part of their official and professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the Council's name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right and copyright must not be compromised when publishing on the Internet. 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.

## **6. Social Media**

- 6.1 Unauthorised posts to Facebook, Twitter, LinkedIn etc could have a detrimental impact on the Council or Councillors or employees and may lead to disciplinary action.
- 6.2 Employees and Councillors should avoid naming the Council or discussing internal council matters on such sites as it could result in the Council being open to legal challenge.
- 6.3 The use of social media must be limited to Town Council business and only authorised employees may use it.

## **7. Intellectual Property Rights**

- 7.1 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). This includes but is not limited to all copyright, design rights, trade marks, 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.
- 7.2 Employees hereby irrevocably and unconditionally waive in favour of the Town Council all moral rights attached to any Service IPR.
- 7.3 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.

## **8. Personal Use of Emails and the Internet**

- 8.1 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**.
- 8.2 ~~ITunes must not be uploaded onto Council software.~~

## **9. Network Security and PC Support**

- 9.1 Employees should not upload or download files from removable storage media without permission of the Town Clerk and the relevant security software being installed on the computer.
- 9.2 Employees should not interfere with the everyday running of the network unless explicitly asked to do so. Any problems with network security should be immediately referred to the IT provider by the Office Administration Manager **and in her absence** the Community Services Manager.
- 9.3 Problems with personal computers should only be referred to the IT provider after reporting to the Office Administration Manager **and in her absence** the Community Services Manager. Employees should not attempt to resolve the problem themselves unless they are absolutely sure of their capability to do so.

9.4 Employees should not have remote access to the server of the Town Council systems without written permission from the Town Clerk

## **10. Enforcement and Remote Monitoring**

10.1 In some cases remote monitoring of websites and/or emails sent by an employee will be monitored, but only in extreme cases where suspicion of illegal behaviour with regard to computer use exists. This may only be carried out under supervision of the Town Clerk. 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 1998.

10.2 Any information obtained from monitoring will be considered by the Council which reserves the right to determine what is and is not suitable.

10.3 Contravention of any of the above regulations may lead to disciplinary action.

DRAFT