

LITTLEHAMPTON TOWN COUNCIL

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS POLICY

1. The Internet

1.1 Introduction

The Internet enables access to valuable information resources in many different formats. The Town Council does not deny legitimate access to information by any member of staff or Councillor, but recognises that such a resource may be open to misuse and abuse. The following policy has been produced in order to safeguard the interests of the Town Council.

This policy sets out the principles underlying the establishment, access and usage of the Internet. It is also designed to ensure protection for both the Council and its employees.

1.2 The Internet & Staff Responsibility

Whilst the Internet contains a wealth of valuable and interesting information, some of this information may be inaccurate, out of date, controversial, offensive and/or illegal.

Littlehampton Town Council accepts no responsibility for the quality, accuracy or availability of information accessed through the Internet. As a user, therefore, it is your personal responsibility to ensure the accuracy of information you discover. Littlehampton Town Council assumes no liability for any loss, damage or injury, direct or indirect, suffered as a result of using these computer resources for Internet access.

1.3 Conditions of Access

All members of staff will be asked to complete a Declaration form stating that they have read and understand this policy document and agree to abide by its terms and conditions.

Personal access will be allowed, but this is firmly restricted and will be monitored accordingly. Staff are allowed to use the Internet for their own purposes but must follow the conditions as applied in the policy statement. The times of access are confined to authorised lunch breaks and after work. It does not include any other time during the working day. After work access must be authorised by either the Town Clerk, Services Manager or Finance & Resources Manager.

1.4 Monitoring

The Town Council may monitor access to Internet sites, and any public access of illegal, offensive or controversial material may be the subject of further action.

1.5 Security

Virus-checking software will run on all computers.

Users may not load/download or install their own software or connect their own computer equipment to any Town Council computer equipment. Exceptions are possible for special equipment to help with general computer use and should be authorised by the Town Clerk, Services Manager or Finance & Resources Manager.

Information from the Internet may be downloaded (within copyright restrictions). To reduce the risk of computer virus infection, all floppy disk, CD/DVD media and memory sticks must be submitted to the Finance & Resources Manager or Town Clerk and checked before usage on any Town Council computer. This does not include new floppy disks and CD-Writable media from the stationery cupboard.

1.6 Prohibited Uses

Littlehampton Town Council does not prohibit specific online activities (other than those listed below) as long as they are not considered to be illegal, offensive, obscene, abusive or troublesome. However, all members of staff should be aware that risks are attached to some on-line activities:

- broadcasting personal or private details over the network may lead to the receiving of unwanted mail or unwanted attention
- on-line financial transactions are an increasingly common use of the Internet and are often conducted safely over secure connections. However, Littlehampton Town Council cannot be held responsible for any losses resulting from sending confidential financial information via the Internet.

Apart from these risks there are a number of activities that are specifically prohibited and must not be undertaken. These include, but are not exclusive to, the following:

- on-line gambling/playing on-line games
- accessing, displaying or disseminating pornography
- posting information that may tend to disparage or harass others on the basis of gender, race, age, disability, religion, sexual orientation or national origin
- participating in chain letters
- posting statements that are defamatory or information that is false or misleading

concerning Littlehampton Town Council or other companies or organisations

- posting confidential or proprietary information about Littlehampton Town Council, its Members or contacts on any Internet sites such as bulletin boards or disseminating such information in a way that might compromise its confidentiality
- downloading, using or distributing copyrighted materials from the Internet without proper authorisation from and/or payment of applicable user fees to the owner of the intellectual property rights of copyrighted materials
- downloading, installing, using or distributing software or executable programs from the Internet without specific permission from the Finance & Resources Manager

The Town Clerk will direct computer users to remove images or text from the screen if, in his judgement, the image or text is inappropriate. Offensive material may lead to disciplinary action for inappropriate use of the Council's internet facility and computers.

1.7 Users must not interfere with equipment or amend or delete existing software.

Staff are not authorised to download software from the Internet for other than specific Council related business use. To ensure the Council's Network is not compromised, any member of staff requiring **ANY** software download facility must contact the Town Clerk, Services Manager or Finance & Resources Manager and confirm a download is required. They will confirm a destination drive and directory for the download; a virus check of the download will be completed prior to releasing the download to the requesting member of staff.

In completing any download you are responsible for ensuring that no software copyright licences are breached.

1.8 Illegal File Sharing

Due to our faster computer networks, staff may be tempted to make illegal downloads of material that is subject to copyright. This includes, but is not confined to, music, film and business software. As this and any subsequent file sharing of this material breaches copyright laws, it is prohibited on any computer that is owned or leased by the Town Council. This also applies to any download or dissemination of material made outside of working hours. Any breach is likely to lead to disciplinary proceedings.

1.9 Penalties for Misuse

The Town Council reserves the right to refuse further Internet access to any individuals accessing or distributing materials which are deemed to be illegal or unacceptable or have the potential to offend or disturb others. The Town Clerk will determine whether any computer activity is unacceptable.

As well as the loss of Internet privileges, other Council disciplinary procedures may be applied, as may criminal prosecution.

Vandalism of, or otherwise intentionally interfering with, the Town Council's computers/ network constitutes a gross misconduct offence and could render the employee liable to summary dismissal under the Town Council's disciplinary procedure.

Logging on to sexually explicit websites or the downloading and/or circulation of pornography or obscene material or using the Internet for gambling or illegal activities constitutes gross misconduct and could render the employee liable to summary dismissal under the Town Council's disciplinary procedure.

1.10 Temporary Staff

From time-to-time, it is possible that the Town Council may need to use temporary staff in order to cover busy periods or annual leave etc. Should any temporary worker need to use a computer as part of their job role, the manager responsible for their day-to-day supervision will be required to bring this policy and its contents to their attention. The temporary worker will need to sign the declaration. It is also Town Council policy that any temporary workers who are required to use a computer will be given their own log-in details. For longer bookings of temporary staff, managers will need to identify if there are any directories or computer files on the computer that will be used that are of a sensitive or confidential nature. If so, the Finance & Resources or Services Manager needs to arrange restricted access to them. The same principles will apply to any self-employed contractors engaged by the Town Council.

2. E-mail, Social Networking & Video Sharing Websites

2.1 Introduction

Most staff also have access to e-mail for exclusive use in connection with the Town Council's business and as part of the normal execution of the employee's job duties. The purpose of these rules is to protect the Town Council's legal interests. Unregulated access increases the risk of employees inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of confidential information. In addition, carelessly worded e-mails can expose the Town Council to an action for libel.

2.2 Usage

As such, e-mails to others outside the Council's staff, such as Members, suppliers, potential suppliers and members of the public, must follow the Town Council's designated house style, which will be supplied to authorised users. Failure to follow the house style is a disciplinary matter and will be dealt with under the Town

Council's disciplinary procedure. E-mail should not be used for unsolicited correspondence or marketing campaigns and employees may not commit the Town Council financially by email unless they have been granted a specific level of delegated authority to do so.

Staff who are authorised users are not permitted to spend time "chatting" by e-mail for personal and private purposes during their normal working hours. Employees are also prohibited from using e-mail to circulate any non-business material.

Staff who are authorised users are also not permitted to log on to Ebay, social networking and video sharing websites such as Facebook, MySpace, Bebo, Twitter and YouTube or use the Council's IT systems to keep a personal weblog ("blog") during their normal working hours. Staff can use these sites during their lunch hour or after work.

Staff should remember that social networking websites are a public forum, even if they have set their account settings at a restricted access or "friends only" level, and therefore they should not assume that their entries on any website will remain private.

Not only does excessive time spent online lead to loss of productivity and constitute an unauthorised use of the Town Council's time, but sexist, racist or other offensive remarks, jokes or pictures sent by e-mail are capable of amounting to unlawful harassment. As "cyber-bullying" is an emerging risk, staff are also prohibited from using the Town Council's electronic communications as a means of intimidating or bullying employees or third parties.

If employees are asked to contribute to an official blog or newsfeed connected to the Council, then the employee will be trained and briefed in detail about what to write.

Employees who are discovered contravening these rules may face serious disciplinary action under the Town Council's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Often web sites ask for a contact e-mail address. Under no circumstances is it authorised that you use your work address for this purpose unless the purpose is strictly on the Town Council's business.

When using email and social networking sites, even in their own time, staff must not:

- publicly identify themselves as working for the Town Council, make reference to the Town Council or provide information from which others can ascertain the name of the Town Council if sending an email not on Council business

- conduct themselves in a way that is detrimental to the Town Council or brings the Town Council into disrepute
- use their work e-mail address when registering on sites unless it is in connection with their work
- allow their interaction on these websites or blogs to damage working relationships between staff and clients of the Town Council
- include personal information, including pictures, about the Town Council's Members, staff, contractors, suppliers or clients without their express consent (an employee may still be liable even if staff, contractors, suppliers or clients are not expressly named in the websites or blogs as long as the Town Council reasonably believes they are identifiable).
- make any derogatory, offensive, discriminatory or defamatory comments about the Town Council, its Members, staff, contractors, suppliers or clients (an employee may still be liable even if the Town Council, its Members, staff, contractors, suppliers or clients are not expressly named in the websites or blogs as long as the Town Council reasonably believes they are identifiable)
- make any comments about the Town Council's staff or Members that could constitute unlawful harassment or bullying
- disclose any confidential information belonging to the Town Council, its Members, staff, contractors, suppliers or clients

2.3 Monitoring

The Town Council reserves the right to monitor employees' e-mails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are :

- to promote productivity and efficiency
- for security reasons
- to ensure there is no unauthorised use of the Town Council's time e.g. that an employee has not been using e-mail to send or receive an excessive number of personal communications
- to ensure the smooth running of the Council's business if the employee is absent for any reason and communications need to be checked
- to ensure that all employees are treated with respect, by discovering and eliminating any material that is capable of amounting to unlawful harassment.

Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private. When monitoring e-mails, the Town Council will, except in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. However, where circumstances warrant it, the Town Council may open e-mails and access the content. In this case, the Town Council will avoid, if possible, opening e-mails clearly marked as private or personal.

The Town Council reserves the right to deny or remove e-mail or Internet access to or from any employee.

3. Use of portable storage devices

3.1 Introduction

Some staff may be provided with portable storage devices, such as memory sticks, that can be plugged into the USB port of a computer. This could include devices used to transfer data from the Town Council's system to a computer used at home but provided or serviced by the Town Council.

3.2 Usage

Whilst they are provided so as to allow for the storage, copying and transferring of files and images between an employee's desktop or laptop computer, their small size and considerable storage capacity makes them vulnerable to misuse. For this reason, any employee issued with these devices must not transfer any data to a third party computer (including one at home) without first having obtained approval from the Town Clerk. From time-to-time, user guidelines will be produced on the usage of such devices and employees will be expected to follow them. Any employee who transfers files to a third party without permission is likely to be subject to disciplinary action and could be treated as gross misconduct.

Employees should also be aware of the terms of the Data Protection Act and the Town Council's Policy with regard to their responsibilities in safeguarding such data, either at work or at home or on other Town Council business.

4. Computer software, games and viruses

4.1 Introduction

The Town Council licences the use of computer software from a variety of outside companies. The Town Council does not own this software and, unless authorised by the software developer, neither the Town Council nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Contravention is a disciplinary matter and will be dealt with in accordance with the Town Council's disciplinary procedure.

4.2 Usage

The Town Council's computer network makes it vulnerable to viruses. Therefore, only duly authorised personnel have the authority to load new software onto the network system. Even then, software may be loaded only after having been checked for viruses by authorised personnel. Any member of staff found to be

contravening this will face disciplinary action under the Town Council's disciplinary procedure.

Employees may not access any computer games.

5. System Security

5.1 Introduction

As many computer files contain some form of confidential or otherwise sensitive business information, the Town Council takes the security of these files very seriously.

5.2 Usage

With this in mind, we have introduced some basic security precautions that all staff must abide by. These are as follows:

- whenever you need to leave your computer for more than a couple of minutes, close the screen or lock your computer, especially if non-staff are around (meetings etc.)
- when creating a computer password, do not use one that is obvious, such as your date of birth or the name of a close family member. All passwords must be reported to the Finance & Resources Manager for protection who will arrange for them to be changed as necessary
- always keep your password private and do not divulge it to any colleague or any outside person
- if you suspect that someone knows your password, change it in consultation with the Finance & Resources Manager
- if you are provided with a Town Council computer for use outside the office, no one else is allowed to use this or its software.

6. Managers

- in addition to the above points, managers will be required to notify the Finance & Resources Manager in advance of any computer users that will be leaving the Town Council's employment. This should be done at least five working days before the employee leaves, so that the individual's account can be closed on their departure
- from time-to-time, the Town Council will review its storage of confidential information and the media upon which it is stored. As part of their job role, all managers will be expected to co-operate in terms of identifying such files, the employees or other staff with access to them and the file locations.

7. Remote Access

Some employees could occasionally spend part of their working week on Town Council business away from the premises. These employees and others who may work remotely on an informal basis should be aware that all aspects of this Policy apply to them.

Remote working employees will also be expected to comply with any additional guidelines that may be introduced in order to reduce the likelihood of the Town Council's computer networks being compromised as a result of remote access.

8. Telephone Misuse

8.1 Introduction

The Town Council's telephone lines are for the exclusive use of employees in connection with the Town Council's business.

8.2 Usage

Whilst the Town Council will tolerate essential personal telephone calls concerning an employee's domestic arrangements, excessive use of the telephone for personal calls is prohibited. This includes lengthy, casual chats and calls at premium rates. Not only does excessive time engaged on personal telephone calls lead to loss of productivity, it also constitutes an unauthorised use of the Town Council's time. If the Town Council discovers that the telephone has been used excessively for personal calls, this will be dealt with under the Town Council's disciplinary procedure and the employee will be required to pay the Town Council the cost of the personal calls made.

Personal telephone calls should be timed so as to cause minimum disruption to the employee's work and should, as a general rule, only be made during breaks except in the case of a genuine emergency.

Employees should be aware that telephone calls made and received on the Town Council's telephone network can be monitored to check that the use of the telephone system is not being abused. If employees wish to make or take a particularly sensitive, private or confidential personal telephone call, they are advised to first advise their line manager of this.

9. Mobile Telephones

Whilst the Town Council will tolerate the use of mobile phones for essential calls during working hours, excessive use for personal calls is prohibited. Also prohibited are lengthy calls, casual chats, text messaging, e-mailing, web browsing

and the taking of video and/or still images (if your phone is so enabled) if not on the Council's business. Your mobile phone should be set to a silent ring during working hours. If you wish to use your own mobile phone, you are requested to do so during official breaks.

Employees of the Town Council who are provided with a mobile phone for use at work are not allowed to use it for purposes other than Town Council business, except in an emergency.

Revised January 2012

This policy will be reviewed regularly to ensure that it remains timely and relevant.