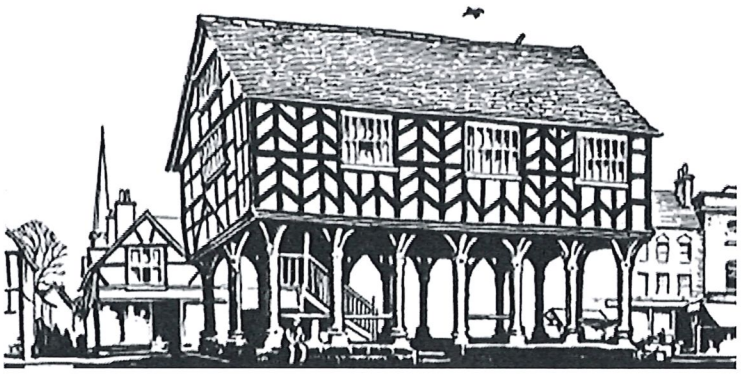
Refer Agenda Item 8.3

21 JUN 2018

LEDBURY TOWN COUNCIL

Ledbury Town Council Acceptable Use Policy



Author: Cllr Jane Hopkins
Version: 1.0
Last Printed: 19/06/201819/06/201819/06/201814:25
Last modified: 15/06/18

Circulation List:
Cllr N Morris, Cllr N Shields

Table of Contents

1 Introduction

1.1 This Acceptable Usage Policy covers the security and use of all Ledbury Town Council's (LTC's) information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all LTC's employees, councillors, contractors and agents (hereafter referred to as 'individuals').

1.2 This policy applies to all information, in whatever form, relating to LTC's business activities and to all information handled by LTC relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by LTC or on its behalf

1.3 This policy should be read in conjunction with the GDPR policy for the control and use of data within LTC.

1.4 It is your responsibility to report suspected breaches of security policy without delay to your line management or The Standing Committee.

1.5 All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with LTC disciplinary procedures.

2 Computer Access Control – Individual's Responsibility

2.1 Access to the LTC IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the LTC IT systems.

2.2 **Individuals must not** allow anyone else to use their user ID/token and password on any LTC IT system.

2.3 **Individuals must not** leave their user accounts logged in at an unattended and unlocked computer.

2.4 **Individuals must not** use someone else's user ID and password to access LTC's IT systems.

2.5 **Individuals must not** leave their password unprotected (for example writing it down).

2.6 **Individuals must not** perform any unauthorised changes to LTC's IT systems or information.

2.7 **Individuals must not** attempt to access data that they are not authorised to use or access.

2.8 **Individuals must not** exceed the limits of their authorisation or specific business need to interrogate the system or data.

2.9 **Individuals must not** connect any non-LTC authorised device to the LTC network or IT systems.

2.9.1 An authorised device is deemed to be IT equipment provided by LTC for staff to undertake legitimate LTC business or equipment provided by current councillors for their use on LTC business.

2.9.2 Council staff must not store LTC data on any non-authorised LTC equipment.

2.10 **Individuals must not** give or transfer LTC data or software to any person or organisation outside LTC without the authority of LTC.

2.11 Line managers and the Standing Committee must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

2.12 Councillors using personal equipment should ensure that no LTC data can be accessed by other family members or other individuals.

This should extend to the storage of LTC data on password protected hard drives or removable storage and never allowing a computer accessing LTC data to be left unattended without a suitable automatic screen-locking mechanism.

3 Internet and email Conditions of Use

3.1 Use of LTC internet and email is restricted to members of staff and current councillors only.

3.2 Use of LTC internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to LTC in any way, not in breach of any term and condition of employment and does not place the individual or LTC in breach of statutory or other legal obligations.

3.3 All individuals are accountable for their actions on the internet and email systems.

3.4 **Individuals must not** use the internet or email for the purposes of harassment or abuse.

3.5 **Individuals must not** use profanity, obscenities, or derogatory remarks in communications.

3.6 **Individuals must not** access, download, send or receive any data (including images), which LTC considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

3.7 **Individuals must not** use the internet or email to make personal gains or conduct a personal business.

3.8 **Individuals must not** use the internet or email to gamble.

3.9 **Individuals must not** use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

3.10 **Individuals must not** place any information on the Internet that relates to LTC, alter any information about it, or express any opinion about LTC, unless they are specifically authorised to do this.

3.11 **Individuals must not** send unprotected sensitive or confidential information externally.

3.12 **Individuals must not** forward LTC mail to personal (non-LTC) email accounts (for example a personal Hotmail account). Except for specified, limited periods when a councillor is unable to receive LTC email.

3.13 **Individuals must not** make official commitments through the internet or email on behalf of LTC unless authorised to do so.

3.14 **Individuals must not** download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.

3.15 **Individuals must not** in any way infringe any copyright, database rights, trademarks or other intellectual property.

3.16 **Individuals must not** download any software from the internet without prior approval of the IT working party, the standing committee or LTC's IT suppliers.

3.17 **Individuals must not** connect LTC devices to the internet using non-standard connections.

4 Clear Desk and Clear Screen Policy

4.1 In order to reduce the risk of unauthorised access or loss of information, LTC enforces a clear desk and screen policy as follows:

4.1.1 Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

4.1.2 Care must be taken to not leave confidential material on printers or photocopiers.

4.1.3 All business-related printed matter must be disposed of using confidential waste bins or shredders.

4.1.4 Confidential materials whether business or staff related should be kept in a locked cabinet when not in use or in a password protected filesystem and should never be left unattended.

5 Mobile Storage Devices

5.1 Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.

5.2 Only LTC authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

6 Software

6.1 Employees must use only software that is authorised by LTC on LTC's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on LTC computers must be approved by the LTC ITC working party.

6.2 Individuals must not store personal files such as music, video, photographs or games on LTC IT equipment.

7 Viruses

7.1 The LTC IT supplier has implemented centralised, automated virus detection and virus software updates within LTC. All PCs have antivirus software installed to detect and remove any virus automatically.

7.2 Individuals must not remove or disable anti-virus software.

7.3 Individuals must not attempt to clean up an infection, without contacting IT support.

7.4 Councillors must ensure their computer systems are fitted with suitable anti virus protection. Councillors must ensure that the anti-virus software and definitions are kept up to date and they should ensure their system automatically scans outgoing emails and that their entire system is scanned regularly.

7.4.1 If a councillor becomes aware of a virus infection they should not send any emails to any LTC address.

7.4.2 They should contact the office by telephone to advise of the infection and the time they believe it will take to correct.

7.4.3 Only when the councillor believes their system is no longer infected should they email any LTC address.

7.5 If an individual receives an email containing a virus from any LTC address they should contact the office who will inform the individual and they should institute the appropriate procedure.

8 Telephony (Voice) Equipment Conditions of Use

8.1 Use of LTC voice equipment is intended for business use. Individuals must not use LTC's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

8.2 **Individuals must not** use LTC's voice for conducting private business.

8.3 **Individuals must not** make hoax or threatening calls to internal or external destinations.

8.4 **Individuals must not** accept reverse charge calls from domestic or International operators, unless it is for business use.

9 Actions upon Termination of Contract

9.1 All LTC equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to LTC at termination of contract.

9.2 All LTC data or intellectual property developed or gained during the period of employment remains the property of LTC and must not be retained beyond termination or reused for any other purpose.

9.3 When a councillor resigns or fails to be re-elected, access to LTC systems must be removed immediately upon receipt of that information. This includes, but is not limited to, changing the Wifi password, changing the alarm code and changing their email password. Any paper documents and keys should also be returned it is the responsibility of the individual councillor to ensure they have complied with this however they will be expected to sign a document indicating that they understand it is a criminal offence not to do so.

10 Monitoring and Filtering

10.1 All data that is created and stored on LTC computers is the property of LTC and there is no official provision for individual data

privacy, however wherever possible LTC will avoid opening personal emails.

10.2 IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. LTC has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

10.3 Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, GDPR 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

10.4 This policy must be read in conjunction with:

10.4.1 Computer Misuse Act 1990

10.4.2 Data Protection Act 1998

10.4.3 GDPR 2018