LEIGHTON-LINSLADE TOWN COUNCIL

ICT Security Policy

Purpose
Leighton-Linslade Town Council is making increasing use of technology in all areas of its services. The information that the Council holds, processes, maintains and shares is an important asset that needs to be suitably protected. The ICT Security Policy sets out an overarching framework in respect of all matters relating to use of electronic data and equipment.

Scope
This policy applies to all information held or owned by the Town Council, any ICT equipment and infrastructure used and the physical environment in which the information/ICT is used.
This policy automatically applies to all Town Councillors, employees, committees and departments. Where access is to be granted to any third party (e.g. contractors, suppliers, volunteers and partners), compliance with this policy must be agreed and documented.

Legal Obligations
The Town Council is required to adhere to legislation including data protection and transparency of information. Full details can be found in the Information and Data Protection Policy.
The Council is required to have in place appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and accidental damage or destruction of personal data.

Policy Framework
A number of policies and procedures exist to safeguard the Council and these must be followed by employees and any others accessing Town Council systems. These include:

Information & Data Protection Policy
Information Security Incident Policy (& Information Security Breach Form)
Removable Media Policy
Use of Internet and Email Policy
Mobile Device User Agreement
Employee Handbook
Password Changing Procedure
Home Working Protocol
Social Media Procedure
Document Retention Policy
Bring Your Own Device Policy

ICT Infrastructure
The physical IT infrastructure of the Town Council will be protected as follows, alongside any other measures deemed appropriate by the Council's IT support provider:

Town Council computers
- Should be shut down properly at the end of each business day
- Users should allow for software updates to be installed when prompted to do so
- Will be maintained by the Council's IT provider to ensure antivirus and other security measures are installed and kept up to date
- May be remotely accessed by the Council's IT provider when necessary
- Software cannot be downloaded onto machines without an Administrator password
- All Town Council work related documentation should be saved on the shared network drive to ensure it is secure and backed up
- Personal or restricted documentation may be saved on an individual's H drive – it cannot be accessed by other staff but will be backed up
- Computer screens should be locked when users are away from their desks

- Monitors should be located appropriately, especially in shared offices or for users likely to access sensitive data

Town Council laptops

- As above, but in addition: laptops should not be removed from Town Council premises except with permission from the Town Clerk or a Head of Service
- Screens should be locked when not in use

Town Council owned mobile devices

- Where appropriate, devices may have pre-installed software on them for security purposes.
- Users of Town Council owned devices must sign a User Agreement outlining terms of use. This includes downloading of software, internet and email use, messaging, pictures and that the device may be subject to audit or inspection.
- Reasonable precautions must be taken by users to ensure security, including password or PIN locking, caution when using freely available WiFi which may be unsecured, caution when installing software or opening messages which may contain links or attachments.
- Screens should be locked when not in use

Server

- Any Town Council servers must be stored in appropriate conditions relating to security, accessibility, temperature etc as advised by the IT support provider.
- The server will be maintained and accessed (either remotely or on site) by the Council's IT support provider.
- Appropriate software such as firewalls, antivirus, antimalware to minimise risk of information loss arising from theft/misappropriation or unauthorised use will be installed and maintained by the Council's IT provider.
- An Uninterruptible Power Supply (UPS) will be installed to prevent risk of disk corruption as a result of power failure.
- The Town Council's IT provider will ensure secure password protection for administrator functions on the server.

Building Security

- Equipment should be stored as securely as possible, within a locked office and a locked and alarmed building.

Data Storage

- The Town Council will ensure secure and robust procedures are in place for the back-up of data from the server and, where appropriate, standalone machines.
- Backed up data will, where possible, be stored off-site or in the Cloud to prevent potential loss.

Network drives

- All electronic information should be saved on the Town Council's network drives rather than on the hard disk of individual machines.
- Access to the Town Council network may only be obtained through the use of a specific user name and password designated by a system administrator.
- Passwords should be changed at least once every six months and should not be disclosed to any other party.
- Where deemed appropriate in the interests of data protection, sensitive and restricted information will be saved in folders on the shared network drive to which access has been restricted to named users. Only the Town Clerk or Head of Democratic & Central Services may request access to restricted drives for specific users.

Email

- All use of email is subject to the Town Council's Use of Email and Internet Policy.
- Where deemed operationally necessary, access to another user's email may be requested through the appropriate channels. This may be temporary, for example in the event of holiday or long term sickness absence. Access should be formally provider to another user rather than the sharing of log-on passwords.
- Use of encryption should be carefully considered if transmitting sensitive or personal information via email. Alternative methods of data sharing may be more secure.

Internet

- All use of internet is subject to the Town Council's Use of Email and Internet Policy.
- Software programmes may not be downloaded from the internet without the authorisation of a systems administrator.

.WiFi

- Personal devices used on Town Council premises are at the responsibility of the owner.
- Town Council staff or guest WiFi may be accessed where available.

Software

- Software may only be installed by the Council's IT support provider or a systems administrator
- Formal licensing agreements must be in place to ensure support is available
- Access to software may be based on the initial user authorisation at log-in or may require additional authentication through a further username and/or password
- Where software is maintained and backed up by a third party provider to the cloud, a clear agreement must be in place, particularly in relation to measures to ensure data security and data protection (compliance with General Data Protection Regulation)

Disposal

All electronic or ICT related equipment must be returned to the Town Council in the event of it being faulty, outdated, no longer required or the user no longer being employed or a member of the Town Council. Electronic equipment will be restored to original factory settings where possible, for future re-use, or all data will be securely removed. Electronic devices will then be disposed of responsibly and securely in accordance with The Waste Electric and Electronic Equipment (WEEE) Regulations 2013.

Training

Despite the growth in targeted cyber crime, it is recognised that the majority of risk occurs as a result of user error. The Town Council has adopted a policy of ongoing training for staff and Councillors. Data protection training is mandatory for all office based staff at least once every three years. In addition to such formal training, it is Council policy to raise awareness of security issues and good practice recommendations on an ongoing basis.

Review

This and related policies will be kept under regular review to take account of new legislation, regulations or business practices.

Adopted by Leighton-Linslade Town Council: 25 June 2018