INFORMATION TECHNOLOGY POLICY

The I.T. Policy and Procedure Manual provides the policies and procedures for selection and use of I.T. equipment owned by the council, which must be followed by all officer and councillors. It also provides guidelines that the council will use to administer these policies, with the correct procedure to follow.

Policy

Wellingborough Town Council uses Microsoft Office 365 for the storage and sharing of data. All staff and councillors are provided with an account which is used for all council business. In adherence with the council's Data Protection Policy no sensitive data should be stored anywhere other than Office 365 (other than statutory requirements for hardcopy minutes), making the council a paperless council.

Council owned Hardware

Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners. The purchase of all desktops, portable computers, computer peripherals and mobile devices must adhere to this policy.

Purchasing desktop computer systems

The desktop computer systems must be purchased through the I.T service provider. The desktop computer system bundle must include:

- Desktop tower, mini Pc or mini tower
- Desktop wide screen with built in speakers
- Wireless keyboard and mouse.
- Microsoft Office 365 with the latest operating system approved by the I.T provider. All PC's will have the following as the minimum specification:
- 2 GHz CPU
- 8 GB RAM
- 5 GB free hard drive space
- Windows 10.
- A minimum of a 1.3 processor, ideally a 1.5 processor

Any change from the above requirements must be authorised by the Town Clerk. The I.T provider will conduct a hardware audit annually and provide recommendations for system upgrades for efficiency.

Purchasing council owned computer peripherals

Computer system peripherals include add-on devices such as printers, scanners, external hard drives etc. Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the council.

Any photocopiers purchased or rented must have the ability to scan to Microsoft Office 365. An agreement must be place with any supplier which provides photocopiers which scan to ensure they are compliant with GDPR and state how they will secure and dispose of the hard disk installed in the device.

Council Software installation on council owned equipment

All software on, including non-commercial software such as open source, freeware, etc. must be approved by the I.T provider prior to the use or download of such software. All users except the Town Clerk and I.T support will be restricted to user access which must require Administrator approval to proceed with any downloads. All purchased software must be purchased through the I.T service provider. The council should maintain a record of the I.T software licence numbers held, and any new licences purchased are to be added to this list. A software upgrade shall only be installed by the I.T service provider. All software must be appropriately registered with the supplier where this is a requirement. Software updates for Microsoft Office will be set to automatically update to enable the effective use of the software.

All computer software copyrights and terms of all software licences will be followed by all Officers and councillors of the council. Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of Town Clerk to ensure these terms are followed.

The I.T service provider should conduct a software audit of all hardware once a year to ensure that software copyrights and licence agreements are adhered to and recommend any software upgrades to improve the council's efficiency.

The Town Council is the registered owner of all software purchased by the council.

Only software purchased in accordance with the getting software policy is to be used on council owned devices.

Prior to the use of any software, the Officer must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All Officers must receive training for all new software relating to their job role. This includes new Officers to be trained to use existing software appropriately.

Officers are prohibited from bringing software from home and loading it onto the council's computer hardware. Software cannot be taken home and loaded on an Officers' or councillors home computer.

Where an Officer is required to use software at home, an evaluation of providing the Officer with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the Officer's home computer, authorisation from the Town Clerk is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the council and must be recorded on the software register by the Town Clerk.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any Officer who makes, acquires, uses unauthorised copies of software or other copyrighted works will be classed as gross misconduct under the council's disciplinary policy.

Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet. All open source or freeware must be compatible with the council's hardware and software systems.

Mobile owned Devices

The purchase of a mobile device must be approved by The Town Clerk prior to purchase. Council owned mobile devices will be assessed annually to ensure that they are able to function with the council's systems and apps. All council owned mobile devices must have a pin code to access the device and a protective case to protect it from breakages. Tracking software will be installed on council owned mobile devices, should the device be lost or stolen device. If any mobile device is lost this should be reported to the Town Clerk immediately for the remote lock and wipe to be performed by the I.T provider.

Mobile devices

Where possible employees should use council owned mobile devices, which should be used to enable public and councillors to contact them when attending to duties outside the offices. This is to minimise the use of personal mobile devices for the transfer or data. Where this is not possible the following personally owned mobile devices are approved to be used for council purposes:

- Mobiles, laptops iPads or netbooks to access wgtc Mircosoft Office 365. Windows, Android or Iphone devices with anti-virus software installed.

Where Wellingborough Town Council emails are accessed, Microsoft Office 365 must be used. The owner of the mobile device must consent to having remote lock and wipe enabled to prevent

the transfer of data, should the device be lost or stolen. If a mobile device is lost or stolen this should be reported to the Town Clerk immediately. All mobile devices must have a pin code or password to access the device. The device must be set to lock after two minutes of inactivity.

Each person who utilises personal mobile devices agrees:

- To make every reasonable effort to ensure that WGTC's information is not compromised through the use of mobile equipment in a public place or by using public WIFI. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.
- To maintain the device with the current operating software and current security software.

- The mobile phones, iPad and tablets must have a pin code set up for access. The phone must be set to lock automatically after 2 minutes of being inactive

- All mobile devices must be set to reject open Wi-Fi or Bluetooth connections without user permission.

- A two-step authentication process must be used for laptops.

- To have a separate log in for other users of the device, to protect the council data access through the device

- To notify Data Protection Officer immediately in the event of loss or theft of the registered device

- Consent to remote lock and wipe the device in the event the device is lost or stolen. Where required support can be provided by I.T to comply with this requirement.

All Officers or councillors who have a registered mobile device for council use acknowledge that the council:

- Owns all intellectual property created on the device and the device must be returned to the council upon them ceasing to be employed or a councillor of the council

- Can access all data held on the device, including personal data

- Will delete all data held on the device in the event of loss or theft of the device

- Has the right to deregister the device for council use at any time.

Data storage

All council data will be stored in Microsoft Office 365. The data will be backed up to the cloud using a compatible Office 365 back up provider. It is the responsibility of I.T provider to ensure that data back-ups are conducted. All sensitive data must be encrypted, and permission rights added to personnel documents. The Town Clerk is responsible for setting permission rights on sensitive data which is emailed or accessed outside the council.

Permission rights must be set on each document, with an expiry date where this information will be restricted from being accessed. Permission rights must also be set to prevent printing or forwarding of sensitive data.

The firewall must be enabled at all times. All council owned PC's and laptops must be encrypted, with a minimum of 256-bit hardware encryption such as Bitlocker 256 bit or similar product.

If removable hard drives and memory sticks are used to transport data, these must have PIN code access with military grade AES 256-bit hardware encryption.

All technology that has internet access must have anti-virus software installed. It is the responsibility of the I.T provider to install all anti-virus software and spam filters on council owned equipment and ensure that this software remains up to date. If there is a suspected security breach, the protocol detailed on this policy must be used and reported to the Town Clerk and I.T service provider immediately.

When viewing sensitive data consideration must be given to ensuring that the content cannot be overseen by people in the vicinity. All information used for council business must adhere to the privacy laws and the council's confidentiality requirements.

Technology Access

Each Officer and councillor are required to set up a secure password to access the council's data. This must consist of upper- and lower-case letters, with at least one number. This must not be shared with any other person.

Where an Officer forgets the password or is 'locked, then the I.T service provider is authorised to reissue a new initial password that will be required to be changed when the Officer logs in using the new initial password.

I.T support will have restricted access to the council's data. This restriction can be lifted by approval of the Town Clerk to provide I.T support. Where the restriction is lifted to the council's data these works must be overseen by an Officer of the council. The restriction must be reinstated after the works have been conducted.

Data Breach
Should the council's data be breached must be reported to the Town Clerk with the following information:

a. What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)
b. How did the breach occur?
c. What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)
d. How many individuals or records are involved? If the breach involved personal data, who are the individuals? (Students, officer, research participants etc)?
e. What has happened to the data?
f. Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)
g. Were there any protections in place? (e.g. Encryption)
h. What are the potential adverse consequences for individuals or the University? How serious or substantial are they and how likely are they to occur?
i. What could the data tell a third party about an individual, what harm could this cause?
j. What commercial value does the information have?
k. What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted)

The I.T provider will provide training on how to recognise a data breach, electronic scams and updates on new cyber risks.

Disposal of equipment
On disposal of council owned devices, the hard drive removed and broken into at pieces. Where devices are owned by contractors an agreement must be put in place for safe and secure disposal of the hard drives on these devices. Personal owned devices used for council businesses must be wiped and or restored to factory settings upon the disposal or the device being transferred to another party. N.B advise should be sought from the manufacturer to determine if the factory reset process is sufficiently secure, and I.T may be contacted for assistance. The Town Clerk must be notified to ensure the council email account is terminated and transferred to the new device. If the device has a removable hard drive this should be removed and broken into pieces to prevent the recovery of data.