THORNBURY TOWN COUNCIL

Councillor IT Policy

Date Ratified:	19 July 2022
Meeting:	Finance and General Purpose Committee
Next review date:	July 2025 *(3 yearly review)*

Contents

1. PURPOSE AND SCOPE

Thornbury Town Council recognises that not all councillors will have equal access to personal IT equipment. The Town Council commits to equipping councillors with the IT equipment to enable them to fully carry out the requirements of the role of councillor. This typically includes:

- To access and respond to emails
- To attend online meetings or training sessions
- To access the summons, agenda and papers for council meetings

It is also the case that some councillors may wish to use their own devices. The requirements for this are set out under section 3 'Bring Your Own Device'.

Town Councillors must comply with this policy where they use a Town Council device, or a Bring Your Own Device, as applicable.

2. PROVISION OF IT EQUIPMENT

2.1 Equipment

Thornbury Town Council will provide the following equipment to councillors who request it in order to carry out the requirements of the role:

1 x tablet device
1 x screen protector/case
1 x keyboard (optional)
1 x mouse (optional)
O365 software

2.2 Request

Requests for IT equipment shall be made to the Town Clerk who shall have delegated authority to place the necessary orders in accordance with this policy.

2.3 Replacement

Replacement shall be on a 4-yearly basis. This may be amended/extended on recommendation from the Town Council's IT provider.

2.4 Appropriate usage

- Councillors should use council issued IT equipment for council business only.
- Councillors will be held liable for the costs of any damage or loss resulting from inappropriate use.
- Councillors will be required to hand over IT equipment on request to Town Council officers, including for the purposes of any necessary IT updates or upgrades.
- Councillors will undertake to adhere to the security requirements set out in the 'Bring Your Own Device' section below.

2.5 Security – Town Council devices

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the Town Council network.

- Passwords must be at least six characters and a combination of upper- and lower-case letters with a number and a symbol.
- Passwords must be kept confidential and must not be shared with family members or third parties.
- Passwords must be changed if it is disclosed to another person or discovered.
- The device must be set to lock itself with a password or PIN if it's idle for five minutes.
- Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
- Public data backup and transfer services (Dropbox, Google Drive) must not be used
- Data must only be stored on internal memory, never on a removable memory cards
- Councillors must hand over the device to Officers on request where there is a personal data breach, a virus, or similar threat to the security of data.
- Councillors must return the device within 48 hours of ceasing to be a Thornbury Town Councillor.
- Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using Wi-Fi facilities in public places (e.g. coffee shops or airports), or Some apps for smartphones and tablets may be capable of accessing sensitive information.
- Lost or stolen devices must be reported to Thornbury Town Council within 24 hours.

3. BRING YOUR OWN DEVICE (BYOD)

3.3 BYOD Introduction

Thornbury Town Council grants Councillors the use smartphones and tablets of their choosing for council business.

This policy is intended to protect the security and integrity of personal data controlled and processed by Thornbury Town Council.

Thornbury Town Council reserves the right to revoke this privilege if Councillors do not abide by the policies and procedures outlined below.

Thornbury Town Council Councillors must agree to the terms and conditions set forth in this Bring Your Own Device (BYOD) policy in order to be able to connect their devices to the Town Council network.

3.4 Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed
- Tablets including iPad and Android are allowed
- Laptops are allowed
- Connectivity issues may be supported by ICT services but this will be on a case by case In the first instance the connectivity issue should be reported to the Clerk
- The device manufacturer or their carrier should be contacted for operating system or hardware related issues.

3.5 Security – Bring Your Own Device

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the Town Council network.

- Passwords must be at least six characters and a combination of upper- and lower-case letters with a number and a symbol.
- Passwords must be kept confidential and must not be shared with family members or third parties.
- Passwords must be changed if it is disclosed to another person or discovered.
- Devices must be encrypted
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Home Wi-Fi networks must be Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
- Public data backup and transfer services (Dropbox, Google Drive) must not be used
- Data must only be stored on internal memory, never on a removable memory cards
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- All data relating to Thornbury Town Council will be erased at the end of a Councillor's term.
- All data relating to Thornbury Town Council will be erased if there is a personal data breach
- All data relating to Thornbury Town Council will be erased if there is a virus or similar threat to the security of data.
- Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using Wi-Fi facilities in public places (e.g. coffee shops or airports), or Some apps for smartphones and tablets may be capable of accessing sensitive information.

3.6 Risks/Liabilities/Disclaimers

- Lost or stolen devices must be reported to Thornbury Town Council within 24. Councillors are responsible for notifying their mobile carrier immediately upon loss of a device.
- Councillors must adhere to the Thornbury Town Council's BYOD policy as outlined above.
- Councillors are personally liable for all costs associated with his or her device.
- Thornbury Town Council reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy

4. DECLARATION

Do you wish to use your own personal IT device for the purposes of Council business: YES / NO

IT equipment issued by the Town Council:

I confirm that I have read, understood and accept the conditions of the Thornbury Town Council IT Policy.

Councillor name: _____

Councillor signature: _____ Date: _____

Witnessed by:

Officer name: _____

Officer signature: _____