Digital Technologies Geelong

Bring Your Own Device (BYOD) Acceptable Use Policy

1. Statement of policy

The purpose of this document is to establish responsibilities, standards and boundaries for acceptable use of BYOD connections to Digital Technologies Geelong (DTG) wireless networks.

Continued access and use of network services is allowed on the condition that each device owner reads, accepts, and adheres to DTG's policies concerning use of BYOD and associated services. The use of a personally owned device in connection with DTG is a privilege granted to device owners through approval of Corporate Information Solutions management. DTG reserves the right to revoke these privileges in the event that device owners do not abide by the policies and procedures set out in this document.

2. Scope

This policy applies to all permanent or part time employees, elected members, contractors, subcontractors, students, guests and third parties who desire connection to DTG's wireless networking infrastructure using personally owned devices.

- Computers
- Laptops
- Smart Phones
- Tablets (IPads etc.)
- Other equipment requiring connection to DTG's wireless network

3. Definitions

The following terms and abbreviations are specific to this policy:
BYOD: "Bring Your Own Device" (BYOD) refers to organisations providing the ability for device owners to bring personally owned mobile devices (e.g. laptops, tablets and smart phones) to the workplace, and use those devices to access privileged organisational information and applications.
User: A member of staff, contractor, visitor, guest or another person authorised to access and use DTG's network.

4. Principles

4.1 Recommended devices

Current devices recommended for Bring Your Own Device use are listed below along with the minimum system requirements:

Devices outside of these specifications do not comply with our policies and system access may not be supported.

4.1.1 Windows laptops

General specifications:

- Intel i5 or similar processor
- 4GB RAM (minimum)
- 250GB (or more) Hard disk drive
- Wireless network adaptor

- Integrated graphics
- Integrated webcam
- Windows 10 or later

High performance specifications:

- Intel i5 or better processor
- 8GB RAM (minimum)
- 250GB (or more) SSD drive
- Wireless network adaptor
- Dedicated graphics
- Integrated webcam
- Windows 10 or later

4.1.2 Macintosh laptops

General Specifications:

- Intel i5 or Intel Dual Core M processor
- 4GB RAM (minimum)
- 250GB (or more) Hard disk drive
- Wireless network adaptor
- Integrated graphics
- Integrated webcam
- OS X 10.14 or later

High Performance Specifications:

- Intel i5 or better processor
- 8GB RAM (minimum)
- 250GB (or more) SSD drive
- Wireless network adaptor
- Dedicated graphics
- Integrated webcam
- OS X 10.14 or later

4.1.3 Mobile Smart Phones and Tablets

- Android 8 or higher Smart Phones and Tablets
- iOS 9 or higher iPhones and iPads
- Windows Mobile 10 or higher

NB: Smart Phones and tablets are only supported for connection to the wireless network.

4.2 Accessible IT services

BYOD's are able to connect to the wireless network via DTG on boarding processes. This requires the user to install security certificates on to their personal device during the on boarding process. Failure to accept the certificate installation will result in the device being disallowed access to the wireless network. Visitors may connect to the guest wireless network without the installation of security certificates although time and bandwidth restrictions will apply.

Connection to the wireless network will provide access to the following services:

- Internet browsing
- Staff Email via Webmail or Exchange where available
- Office365

- OneDrive Storage – via Office365
- Virtual Desktops and Applications (Where available)

4.3 Corporate Information Solutions support

Corporate Information Solutions at DTG does not support or maintain operating system or hardware related issues for BYOD.

DTG will not cover any impairment of the device that may have occurred whilst connected to DTG network.

DTG does not take responsibility for any loss, theft or damage to a BYOD the user elects to use on DTG premises. The device owner is personally liable for the device and any carrier service costs that may be incurred.

Corporate Information Solutions will provide assistance in connecting the BYOD to the wireless network where the user is not able to follow the instructions provided on the staff portal or where the on boarding process fails. Wireless network connection issues that are directly related to the user's hardware, installed software or operating system anomalies are not supported by Corporate Information Solutions.

Devices that have been subject to "jailbreaking" in the case of an iPhone or "rooting" in the case of android devices are not supported.

4.4 Device owner responsibilities

The device owner carries specific responsibilities, as listed below:

- All users of DTG wireless network must read, understand and adhere to the Network User Policy prior to accessing the network with a BYOD.
- In order to access DTG network and associated resources using a personal device a user will be required to enter a valid network account username and password.
- Users will not provide network username and password details to any person or share any device that is connected to the wireless network with an individual username and password.
- Staff must not use their device to store corporate e-mails, files and data. All corporate data must be stored on the allocated network shares. DTG shall not be held responsible for any loss of data stored outside of the provided network locations.
- Staff must not store DTG data on personal cloud services. (I.e. Dropbox, Box, Google Drive etc.)
- Backing up personal or work-related files on BYOD's is the responsibility of the device owner.
- The policy may require the use of a four-digit pin to successfully on board your mobile device. Acceptance of the pin is mandatory in these cases.
- BYOD owners are responsible for the safekeeping of their personal devices at all times.
- BYOD owners will make every reasonable effort to ensure that their device has appropriately updated virus protection, in addition to the application of all current security and critical vendor supplied operating system patches.
- No BYOD owner shall establish a wireless ad-hoc or peer-to-peer network using a personal electronic device or any other wireless device while on institute property.
- In addition to the above, all users are expected to use their device in an ethical manner. The use of a BYOD which in any way breaches the Network User Policy is not permitted and may result in disciplinary action.

DTG reserves the right to refuse, prevent or revoke connection to DTG network without notification for breaches of responsibilities contained within this policy or related policies.

4.5 DTG responsibilities

DTG responsibilities include:

- Ensuring that the availability and stability of DTG wireless network meets or exceeds the existing Service Level commitments.
- Ensuring that BYOD users have access to internal and external resources required to complete employment obligations.
- DTG must also remain mindful of the personal usage of such devices and the privacy of the individual. DTG will not monitor the content of your personal devices; however, DTG does reserve the right to log and monitor traffic transferred between your device and DTG systems, over both internal networks and access from remote locations via the internet.
- In exceptional circumstances, for instance where the only copy of a DTG document resides on a staff members personal device, or where the Institute requires access in order to comply with its legal obligations, or where obliged to do so by a Court of law or other law enforcement authority, DTG may require access to information stored on your personal device. Under these circumstances, all reasonable efforts will be made to ensure that DTG does not access your private information.
- DTG has a duty of care in ensuring that employees are not subject to inappropriate content whilst connected to DTG network, therefore all BYO devices connected to the wireless network will be subject to DTG's internet filters in the same manner as domain-connected devices.

5. Governance / responsibilities

POSITION	GOVERNANCE / RESPONSIBILITY
Corporate Information Solutions	For providing secure and consistent access to the Institute network to enable staff and students to meet obligations of employment and study. This responsibility extends to the provision of IT systems for staff and students who elect to bring their own devices to achieve required occupational and educational outcomes.
Users of the network	For adhering to policy and ensuring compliance with the intent of this policy.

6. Key aligned internal documents

Network User Policy IS PO 03

7. Review and approval

	POSITION	AREA
Business Process Owner	Chief Information Officer	Corporate Information Solutions
Endorsed by (if applicable)	Nil	
Ratified by (if applicable)	Nil	
Review schedule	This policy will be reviewed every year (or earlier as required)	
Last reviewed / updated	23 June 2021	