

# BYOD for Registered Training Organisations

# Sample Policies

****

[flexiblelearning.net.au](http://flexiblelearning.net.au)

These sample policies are designed for use by Registered Training Organisations. They are intended to act as a guide only. Care should be taken to delete any policies that are not applicable, as well as to customise the wording and details within the policies so that they are appropriate for use in individual RTO contexts.

# 1. Bring Your Own Device Policy

The increased ownership of personal electronic devices requires that *(organisation name)*, learners, employers and parents take steps to ensure that personal electronic devices are used responsibly. This policy is designed to ensure that potential issues can be clearly identified and addressed and that individuals’ own devices can be effectively and safely used for optimal learning and productivity outcomes.

# 2. BYOD Policy - Learners

This document sets out the conditions for Bring Your Own Device (BYOD) at *(organisation name)* for learners. These devices include smart phones, tablets or laptops with the capability of connecting to the *(organisation name)* wireless internet and/or internal network for the purposes of study and work. Once connected, you will have access to (*delete where non-applicable)*:

* The internet
* The Learning Management System
* RTO resources, such as the library portal, web printing and email

## Acceptable BYOD Use

* The use of learners’ own devices whilst connected to the *(organisation’s)* network is governed by the Acceptable Use Policy.
* Electronic devices must be switched to “silent” mode during class times and professional etiquette demonstrated at all times, with respect to phone calls, sending and receiving SMS, email or other messaging types.
* Students should not transmit or show material of an offensive nature.

## Safe use and device security

* You are responsible for the maintenance and upkeep of your device. *(Organisation name)* does not accept responsibility for replacing or repairing lost, stolen or damaged personal electronic devices belonging to learners.
* Personal devices should be marked clearly with your name.
* Always store your device in a protective cover and follow the manufacturer’s instructions for care and maintenance.
* Do not leave your device unsupervised.
* It is strongly advised that you use a password or pin on your device to deter unauthorised use of your device. This password or pin should be kept secret.
* Keep yourself and others safe by not giving out personal details to unknown sites or individuals.

## Virus Protection

You are advised to:

* Protect your devices from virus attack by keeping your operating system and antivirus software up-to-date.
* Consider running virus scans regularly after accessing the internet or personal email.
* Exercise due caution when downloading files from the internet.

## Power supply and battery management

* You must bring your device fully charged at the beginning of the day as *(charging on campus is not permitted / access to charging facilities is limited).*
* You must bring your own power supply if you need to charge your device as ICT or other staff will not be able to lend you recharging facilities.

## Backup and/or recovery

* You are responsible for your own backup of critical data at all times. This may be through the use of a USB, external drive or internet-based backup to regularly back up important work. Any lost work is your responsibility and it is strongly advised that you take precautions to avoid this problem.

## Software and applications for learning

* You may be required to purchase and/or download and install specific software/ applications (“apps”) onto your device in order to access your learning materials. This will be at your own expense.
* You will need access to a relevant online Application Store (e.g. Apple App Store, Google Play Store) account associated with your device in order to download most applications.

## Software and application updates

* You are responsible for regularly applying updates for any software or applications (“apps”) needed for the purposes of learning prior to attending scheduled classes. This may be undertaken while connected to the *(organisations)* network, provided this is outside of class time.

# 3. BYOD Policy – Staff members

This document sets out the conditions for staff Bring Your Own Device (BYOD) at *(organisation name)*. These devices include smart phones, tablets or laptops with the capability of connecting to the *(organisation name)* wireless internet and/or internal network for the purposes of study and work.

Once your device has been registered on the *(organisation)* network, you will have access to (*delete where non-applicable)*:

* The internet.
* The *(Organisation name)* Learning Management System.
* RTO resources, such as the library portal, web printing.
* *(Organisation name)* intranet and email.

## 3.1 Acceptable BYOD Use

* The use of staff member’s own devices whilst connected to the *(organisation’s)* network is governed by the Acceptable Use Policy.
* Professional etiquette is to be demonstrated at all times, with respect to phone calls, sending and receiving SMS, email or other messaging types while on campus.
* Staff must not transmit or show material of an offensive nature.

## Safe use and device security

* You are responsible for the maintenance and upkeep of your device. *(Organisation name)* does not accept responsibility for replacing or repairing lost, stolen or damaged personal electronic devices belonging to staff members.
* It is advised that you add coverage for loss, theft or breakage of your mobile devices to your contents insurance policy.
* Personal devices should be marked clearly with your name.
* Always store your device in a protective cover and follow the manufacturer’s instructions for care and maintenance.
* Do not leave your device unsupervised.
* It is essential that you apply a password or pin on your device to deter unauthorised use of your device and keep sensitive information. This password or pin should be kept secret.
* Keep yourself and others safe by not giving out personal details to unknown sites or individuals.

## Device loss or theft

* In the event that your device is lost or stolen, you must advise *(relevant staff member – e.g. ICT manager, training manager, administration manger)* immediately. This is in order to prevent any sensitive personal, student or client data being misused.
* In the event that your device is lost or stolen, a remote wipe will be applied to your device to protect sensitive information. This will permanently delete all data on your device, including personal data.
* It is highly recommended that you back up all content on your device, including personal photographs, notes, videos and documents to an alternate storage mode, such as in the cloud, or a hard drive or USB.

## Virus Protection

You are advised to:

* Protect your devices from virus attack by keeping your operating system and antivirus software up-to-date.
* Consider running virus scans regularly after accessing the internet or personal email.
* Exercise due caution when downloading files from the internet.

## Power supply and battery management

* You must bring your own power supply if you need to charge your device as ICT or other staff will not be able to lend you recharging facilities.
* Charging devices should be undertaken with due regard to Workplace Health and Safety considerations.

## Backup and/or recovery

* You are responsible for your own backup of critical data at all times. This may be through the use of a USB, external drive or internet-based backup to regularly back up important work. Any lost work is your responsibility and it is strongly advised that you take precautions to avoid this problem.

## Software and applications for learning

* You may be required to purchase and/or download and install specific software onto your device in order to access resources related to your work.
* You will need access to a relevant online Application Store (e.g. Apple App Store, Google Play Store) account associated with your device in order to download and install most applications.
* You will need to ensure that your device has enough free storage space to enable you to install and run the requisite applications and programs to accomplish your work.

## Software and application updates

* You are responsible for regularly applying updates for any software or applications (“apps”) needed for the purposes of training and assessment. This may be undertaken while connected to the *(organisations)* network.