

Policy: Technology devices usage

‘Building Digital Capacity’ resources series

 

This resource is licensed by Community Legal Centres Queensland Inc under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0). To view a copy of this licence, visit <https://creativecommons.org/licenses/by-sa/4.0/>.

|  |  |  |
| --- | --- | --- |
| **Resource type:** | **Strategic area:** | **Use it to:** |
| Policy template |  | * Adapt the policy to your CLC and help your team make appropriate use of the devices available to them including computers, phones and tablets.
 |

*Current as of February 2020*

HOW TO USE THIS POLICY

* Copy pages 3 and 4 of this document and use this template as a guide for your organisation, replacing [text in brackets] where applicable (you can do a Find & Replace on ‘[CLC name]’).
* Review the policy content and make amendments as required for your centre. Adjust formatting, title, footer, etc. as needed.
* Once this policy document is completed, share the policy with your users, i.e. staff members as well as volunteers if they access your systems.
* Ensure all your digital and technology-related policies are easily accessible to your users. This could be your local shared drive, your intranet, or any cloud-based document sharing software in use for your centre like Google Drive, SharePoint or Dropbox.
* Ensure all new starters (staff and volunteers) receive a copy of the policy as part of their induction process.
* Finally, ensure the policy’s latest version is distributed when updates are made.

technology devices usagePOLICY TEMPLATE

WHAT this policy is for:

This policy describes [CLC name]’s acceptable usage of computers, phones and devices, including use of teleconference phone numbers. This includes maximum reimbursements of phone expenses.

WHO this policy is for:

All staff, temporary employees, contractors, volunteers and management committee/board members of [CLC name], collectively described as ‘users’.

Who is responsible for what:

* [CLC name] is responsible for providing all its users with the appropriate electronic, computing and telecommunications devices and resources: all IT facilities owned or leased by [CLC name] are provided to assist users to conduct bona fide professional activities.
* All users must accept full responsibility for using IT equipment and resources in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people.
* Users are responsible for looking after the equipment allocated to them, including keeping that equipment secured through appropriate use of passwords, screen locks, physical lockers, and other security mechanisms.
* Users have a responsibility to promptly report the theft, loss or unauthorised disclosure of [CLC name]’s equipment and proprietary information.

The do’s and don’ts:

**Acceptable usage:**

* IT equipment and facilities must be used primarily for the purpose of professional activities. Use of facilities for leisure or personal purposes (e.g. sending and receiving personal emails, making a personal phone call, browsing the internet, excluding video streaming or movies downloads) is permitted so long as such use does not incur specific expenditure for [CLC name], impact on job performance, break the law, or bring [CLC name] into disrepute.
* Fixed phone lines should be used whenever possible in preference to mobile phones for calls not covered under the mobile phone plan (e.g. special numbers, international calls, once monthly mobile quota has been reached).
* Mobile phones may be used to the authorised reimbursement limit, which covers phone calls, text messages and data downloads.
* Personal calls/data usage must not exceed [10%] of usage and/or [1.5GB] per month.
* Teleconference numbers may be used for calls involving 3 or more participants in different locations. For calls involving 2 participants, standard phones lines must be used.
* Only authorised personnel may access specialist equipment like servers and networking equipment.

**Unacceptable usage:**

* All [CLC name] computing or networking equipment, software or IT facilities, including email and web servers and other similar resources, may not be used for any action that hinders legitimate computer usage, creates unnecessary work for others or invades the privacy of another person or organisation. These actions include the following:
* attempting to create or install any form of malicious software (for example worms, viruses, Trojan horses, etc.);
* creating or transmitting any material or data which could reasonably be deemed abusive, offensive, defamatory, obscene or indecent, or harass, intimidate, harm or distress others;
* creating or transmitting materials that infringe copyrights of another organisation or person;
* conducting unauthorised commercial activities for personal or financial gain;
* deliberately accessing or attempting to access unauthorised materials, information, services or facilities;
* tampering with or moving installed IT equipment or facilities without authorisation.