

Policy: Internet, social media and email usage

‘Building Digital Capacity’ resources series

A close up of a logo

Description automatically generated A drawing of a face

Description automatically generated

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 internet, social media and email. |

*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.

Internet, Social Media and email usage AND EXIT POLICY TEMPLATE

WHAT this policy is for:

This policy describes [CLC name]’s acceptable usage of internet, social media and email; how users are permitted to access and download information from the internet; manage and publish [CLC name]-related content through websites and social media; and communicate via email.

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] encourages the use of the internet, including email and social media, to facilitate communication among internal users and with our external community and stakeholders to allow users to better perform the duties assigned to them.
* [CLC name] is responsible for providing its staff, temporary employees, contractors and volunteers with access to the internet, email and, for authorised users, to official social media accounts (Facebook, Twitter, LinkedIn, YouTube, Instagram, etc.).
* Users are responsible for using email, social media and internet services in accordance with [CLC name] policies and procedures of ethical conduct, safety and compliance.

The do’s and don’ts:

**Acceptable usage:**

* Each user is allocated an individual [CLC name] account, except for users like volunteers who may share a generic account. This email account should be used primarily for [CLC name] professional duties and related purposes. Personal communications are permitted on a limited basis, but not for a personal commercial use or any use that could compromise [CLC name] relationships and activity.
* Personal internet use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch. Personal internet use must not affect the internet service available to other users (especially non-work related internet activities that involve bandwidth heavy uses).
* All [CLC name] data contained within an email message, including attachments, must be in accordance with the [CLC name] *Information Security, Data Protection and Privacy Policy*.
* Users must use an email signature conform to [CLC name]’s standard: [if available, insert the signature standard in this section].
* Users are representatives of [CLC name] when using their [CLC name] email address or social media accounts, and as such must display professionalism, respect and courtesy in all their online communications, and ensure these communications are in the interest and spirit of [CLC name].
* Comments made by any user through social media or emails are a part of public statements made on behalf of [CLC name]. As such, employees and other users are to comply with any delegations or procedures covering the use of the media and are to confirm with their manager that the topic they wish to address does not have any legal aspects or other sensitivities that need to be taken into account before making public statements.
* Authorised users of social media accounts must use these in a safe and responsible manner.

**Unacceptable usage:**

* Users may not email, upload, post, download, or browse websites containing materials (text, images, videos and other digital content) that could reasonably be deemed abusive, offensive, defamatory, obscene or indecent, or harass, intimidate, harm or distress others; or infringe the law.
* Users are not permitted to post, upload or share [CLC name] information using a social media account unless designated as authorised users of those social media accounts.
* Authorised users of [CLC name] social media accounts must not post any content (text, images or other media) that may be deemed inappropriate such as pornography, racial or religious slurs, gender-specific, offensive or discriminatory comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.
* Users must not send bulk or mass emails, particularly to external parties, using their standard email software [specify email software used, like Gmail or Outlook]. Mass emailing is strictly limited to authorised users and must be carried out with the designated, approved digital marketing tools [specify emailing tool used like Mailchimp or Campaign Monitor].
* Users must not download or open suspicious attachments from emails or websites, or open links in documents unless you were expecting it as part of your work, and should report any suspected virus or malware to their local IT support or supervisor.