

Policy: User set up and exit

‘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 manage staff and volunteers access to your CLC systems.
 |

*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.

USER SET UP AND EXIT POLICY TEMPLATE

WHAT this policy is for:

This policy describes how new [CLC name] staff, volunteers and management committee/board members should be granted user accounts and access to relevant systems, and actions required upon user exit.

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 ensuring prompt and efficient setup of information and communications technology (ICT) systems user accounts, access and equipment for new users.
* [CLC name] is responsible for ensuring prompt and efficient decommissioning of ICT user accounts, access and equipment for users leaving the organisation.
* New users are responsible for following the ICT induction training and instructions provided to them, and familiarise themselves with the [CLC name] ICT environment, policies and systems they will be using in their roles.
* Users leaving [CLC name] are responsible for handing over their equipment and devices including accessories, leave their data in good order and in the appropriate location, and helping with the transfer of email, data and documents to the appropriate recipient (either a supervisor, a colleague, an incumbent or an administrative user).
* [CLC name] ICT support is responsible for removing access to all system accounts allocated to that user.
* The user’s immediate supervisor is responsible for authorising requests for access to systems and ensuring removal of accesses are processed upon user’s exit.

The do’s and don’ts:

**Acceptable usage:**

* The immediate supervisor of the new or departing user can submit a request for user set-up or user account decommissioning up to 5 days before the user starts or leaves.
* When a user leaves, their supervisor must ensure their data and documents are transferred to another person: in particular, supervisors should request from ICT support for that person’s documents, files and emails to be transferred upon leaving.
* Volunteers accessing systems should be given only access to data and functionalities they require to perform their activities.
* Volunteers should be given their own login where possible. Generic logins (e.g. admin@clc.org.au or volunteer@clc.org.au) should be avoided for any systems that involve either access to personal data or changes to data that may need to be tracked (e.g. CLASS).

**Unacceptable usage:**

* Users leaving the organisation are not permitted to take any device, information or data, belonging to [CLC name].
* Users leaving the organisation are not permitted to access, or attempt to access, systems or applications owned or used by [CLC name].