

CCIMDC18042019	Information Technology Policy
----------------	--------------------------------------

Access4u is committed to ensuring that the work of staff is supported and assisted by integrated and efficient information technology.

As far as possible within available resources, Access4u will maintain an up to date computer system providing staff with:

- reliable software for their day to day tasks
- high speed internet access
- personal email and messaging systems

Responsibilities and delegations	
This policy applies to	Governing Body, CEO/Managers/Staff and Volunteers
Specific responsibilities	<p>The Board – Ensure an integrated and efficient information technology.</p> <p>CEO – Ensure computer access up to date and reliable with access to email and messaging systems.</p> <p>Staff – All staff utilising business related information technology for business purposes.</p>
Policy approval	CEO

Policy context – this policy relates to:	
Standards	NDIS Practice Standards National Standards for Disability Services
Legislation	The Privacy Act 1988 (cth) and 13 Privacy Principles
Contractual obligations	NDIS Provider Registration Individual Participant (Client) Service Agreements
Organisation policies	Privacy and Confidentiality Policy Access to Confidential Information Client Records Mobile Phone and Computer, Internet and Email Usage Policy and Procedure
Forms, record keeping, other documents	Management Information and Monitoring

Procedures

IT Equipment and responsibilities

The organisation maintains the following computer system:

- Laptops

- Desktops
- Tablets
- Mobile phones

All the devices provided by YNA ITS is networked and have the standard configuration compliant to YNA Domain controller.

Users permission and access to file and folders are custom built and are defined by the CEO of the organisation and built in-house by YNA ITS technicians.

- All users are provided restricted access for data files defined by their manager, the files are hosted in-house on the dedicated server onsite.
- Any new software installation needs to go through initial audit by YNA ITS technicians.

The YNA ITS is responsible for:

- maintaining the system and liaison with IT contractors or technicians when necessary
- providing advice to the organisation regarding IT issues
- providing an IT orientation to new staff members
- providing IT support to staff

Information management and access

The system consists of:

Access4u has a dedicated shared drive for all users, it is defined O: (network drive)

Filing and naming protocols

-NA- as defined by the manager of the department.

Information security

YNA ITS use a cloud-based antivirus application which regularly gets updated based on the push update by the vendor. YNA ITS monitors every push update by the vendor when it happens.

YNA ITS is responsible for the back-up of files on the data file server. We take 60-minute incremental back-up of data files on our primary data server which is kept up to 30 days.

Our current back-up storage is hosted off-site at 246 Glen Osmond Road, Fullarton

YNA ITS conducts test restoration of data on a quarterly basis.

Staff doing computer-based work from home must have adequate virus protection software installed on their home computers, and ensure that any files transferred to the organisation's computer system have been virus screened. Users are expected to be responsible for the security of any company devices taken offsite.

Accidental loss of data

YNA ITS is only responsible for files on the data file server. We have a 60-minute incremental back up of data files which is kept up to 30 days. It is important all data is saved on to the server rather than the users device. YNA ITS do not take any back up of the local data.

Use of internet

Use of the organisation's computer network to access the internet for personal use is permitted, provided it conforms to the organisation's policy on personal use of organisational resources.

This prohibits use of the network to:

- access pornographic, gambling or gaming related sites or material
- use EBay or similar online purchasing sites or 'dating' sites
- create or exchange messages, images or sounds that are offensive, harassing, defamatory, obscene, sexually harassing or threatening
- download any files without permissions for intellectual property rights (including commercial software, games, music or movies)
- create or exchange advertisements, solicitations, chain letters and other unsolicited or bulk email
- download software without the approval of YNA ITS
- play games in work time

Staff should also ensure that any activity on a personal social network site does not identify or implicate Access4U in any way and that organisational policies regarding confidentiality and privacy are extended to all internet exchanges.