INTERNET, EMAIL AND COMPUTER USE POLICY.

CONSIDERATIONS	LEGISLATION
Code of Conduct	Copyright Act 1968 (Cth)
Discipline and termination policy	Disability Discrimination Act 1992 (Cth)
Privacy Policy	Equal Opportunity Act
Sexual Harassment policy	Fair Work act
Workplace Health & Safety Policy	Privacy Act 2013
	Racial Discrimination Act
	Sex discrimination Act
	Trade Practices Act

1 PURPOSE

THE Chester hill Neighbourhood Centre recognises the usefulness of the internet, email, mobile devices and computer equipment as research, communication and work tools. This policy sets out the appropriate standards of behaviour & ethics for users of the organisations information technology resources

2 INTRODUCTION

At all time when accessing or using CHNC information technology resources, users must ensure that they comply with this policy. It is the user's responsibility to ensure that they use the Centres information technology resources in a lawful and professional manner.

This policy outlines the expectations in the use of the Neighbourhood Centres

3.1 Information Technology resources

3.2 Internet

3.3 Social Media

3.4 Email facilities

3.5 Mobile Phone and mobile devices

If the user is unsure about any matter covered by this policy, they should seek the assistance of the manager or their coordinator

2.1 SCOPE

This Policy applies to all Management Committee &staff members of CHNC, Volunteers, clients and contractors, referred to as users.

This policy applies to the use of all internet, email, computer facilities(including laptops, mobile phones and similar products) , both during and outside of business working hours, inside the workplace and as well as from remote locations.

3.1 INFORMATION TECHNOLOGY RESOURCES

Chester Hill Neighbourhood Centres information technology resources are provided to support the business and administrative activities of the organisation.. These resources include

- The Neighbourhood Centres Network
- Computer systems and software including personal computers, notebooks and servers.
- Mobile phones, smart phone and wireless data cards
- Access to the Internet
- Email, telephones and related services

If users produce, collect and/or process organisation related information in the course of their work, that information remains the property of Chester Hill Neighbourhood Centre

3.1.1 Extent of personal use

Users are permitted to use the organisations IT resources for limited, incidental personal purposes, provided that such does not:

- Interfere with the efficient business operations of the organisation
- Violate the policy or any other policy of CHNC
- Negatively impact upon the user's work performance
- Obstruct the work of other users
- Damage the reputation. Image or operations of CHNC
- Such use must not cause noticeable additional cost to the organisation
- CHNC accepts no responsibility for

Loss or damage or consequential loss or damage, arising from personal use of its IT resources

Loss of data or interference with personal files arising from the efforts to maintain the IT resources

3.1.2 Guidelines for use of IT resources

Users must comply with the following guidelines when using CHNC IT resources:

- Users must use their own username/login code when using CHNC computer system, unless authorised . (eg admin for Social support and CVS)
- Users should protect their username/login and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.
- Username/login codes and passwords are not to be recorded on or near computer equipment/mobile devices
- Users should ensure that they log off from their account, and lock their computer /mobile device or shutdown their computer/ mobile device when leaving such equipment unattended to ensure that others do not have access to CHNC computer system
- Users in possession of CHNC computer equipment or mobile devices (including laptops & mobile phones) must at all times ensure that such equipment is stored or placed in areas with minimal possibility of theft or damage.
- CHNC IT resources must not be used for private commercial purposes.
- Use of proprietary software is subject to terms of licence agreements between CHNC and the software owner, and maybe restricted in its use

3.1.3 Prohibited conduct

Certain behaviour is considered to be inappropriate use of CHNC IT resources and is strictly prohibited/ Examples of such prohibited conduct are, but not limited to:

a) Users must not send (or cause to be sent) upload, downloads, use, retrieve, or access any file, email or internet material that:

1. Is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to an internet site (URL). For example, material of a sexual nature, hateful, indecent or pornographic material.
2. Causes insult, offence, intimidation or humiliation by reason of unlawful harassment or discrimination.
3. Is defamatory or incurs liability or adversely impacts on the image of the organisation. A defamatory message or material in a message or material that is insulting or lowers the reputation of a person or group of people.

4. Is otherwise illegal, unlawful or inappropriate.

5. Affects or may affect the performance of, or cause damage to or overload CHNC computer system or internal or external communications in anyway

6. Gives the impression of or is representing, giving opinions or making statements of or on behalf of the organisation without the express authority of the organisation.

b) Users must not use IT resources to:

1. Violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied. Users should not copy or access copyrighted music or videos on the organisations IT resources

2. Create any legal or contractual obligations on behalf of CHNC unless expressly authorised to do so.

3. Disclose any confidential information of CHNC or any employee, volunteers or client unless expressly authorised to do so.

4. Install software or run unknown or unapproved programs on CHNC computers. Under no circumstances should users modify the software or hardware environments of CHNC computer system (this includes installing software purchased by users for private use) without prior approval.

5. Gain unauthorised access (hacking) into any other computer within the organisation or attempt to deprive other users of access to any of CHNC computing system.

6. Plagiarise another persons work

7. Deliberately send or cause to be sent chain spam emails in any format.

8. Obtain personal gain. For example, running a personal business using CHNC computers or resources.

9. Gamble

10. Stream content for personal use.

11. Download, install or use instant messaging soft ware.

12. Perpetuate any form of fraud or software, film or music piracy.

c) Users must not use another users computer or internet access or email facilities (including passwords and usernames/login codes) for any reason without the express permission of the user

3.2 Internet

CHNC resources should only be connected to the intern et using authorised means.

Users are not permitted to publish personal web pages on computers connected to CHNC systems.

3.3 Social Media

Staff members are not permitted to "recommend" their current or former co workers for professional networking sites which would identify CHNC as the users employer (such as "LinkedIn") without prior approval.

CHNC IY resources are provided for work purposes. Access to social networking websites is not deemed a requirement of most positions. However if a uses is permitted to access social media websites, the user us responsible for ensuring that their access does not:

- Interfere with the efficient business operations of CHNC
- Violate this policy or any other policy of the organisation
- Negatively impact upon the users work performance
- Hinder the work of other users
- Damage the reputation, image or operations of CHNC

For the sake of clarity, social media includes, but is not limited to, Social networks (such as Facebook and Myspace), BLOGS, Wikis (such as Wikipedia), Podcasts, Forums, Content communities (such as YouTube and Flickr), Microblogs (such as Twitter)

Users must take a common sense approach to the content that they publish online. Because of the public nature of the internet and social media, this common sense approach also applies to use of social networking sites outside of business hours or on equipment other than CHNC.

Is the user is holding themselves out as a representative of CHNC, any material published online must:

- Be relevant to the users area of expertise
- Not be anonymous
- Maintain professionalism, honesty and respect

Statements of fact about CHNC and its services, publicly available information and information already published on the website are all examples of appropriate online content.

Users must not publish any material online that contains CHNC confidential information (including financial information and information about organisation matters), the personal information of another (without that individuals consent) information about clients or volunteers, or information that may offend, intimidate, defame of humiliate staff, volunteers or clients of CHNC. Is a user becomes aware of inappropriate use they should report such conduct to the Management Committee or Manager of CHNC.

3.4 Email

Appropriate standards of civility should be used when using emails and other messaging services to communicate with other staff members or any other message recipient. When using the email or messaging system users must not send:

- Angry or antagonistic messages- these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures.
- Offensive, intimidating or humiliating emails- CHNC IT resources must not be used to humiliate, intimidate or offend another person/s on the basis of their race, gender, or any other attribute prescribed under anti discrimination legislation. Users must not include names, personal numbers or addresses of staff in emails.

3.4.1 Guidelines for use of CHNC email system

A user must comply with the following guidelines when using CHNC email system:

- Any disclaimer which is automatically included in CHNC emails must not be removed.
- Is a user receives an email which they suspect contains a virus, they should not open the email or any attachment to the email and should immediately contact Management for assistance.
- If a user receives an email which includes an image, text, materials or software that is in breach of CHNC policy, the user should immediately delete the email and report the matter to the Manager. The user must not forward the email to another person.
- Users must not publish their CHNC email address on a private business card.
- Users must not forward or copy emails that contain personal information about an individual without the prior permission of that individual.
- Users must adhere to the guidelines and prohibitions set out in this policy at all times.
- Separate guidelines will be included in Memorandums of Understanding or contracts between partnerships eg CHNC CVS and Bankstown Uniting Church CVS where information is shared.

3.5 Mobile phones and mobile devices

Mobile phones and or mobile devices may be provided by CHNC for the purpose of carrying out CHNC business. The devices (including telephone numbers) remain the property of CHNC at all times. Mobile phones and mobile devices are considered IT resources and as such their use if governed by this policy and should ensure that the devices are used in the most cost effective manner. An investigation may be undertaken when it id identified that a uses is exceeding reasonable personal use of the equipment provided.

3.5.1 Guideline for use of CHNC mobile phone and mobile devices.

Users must comply with the following guidelines when using CHNC mobile phones and mobile devices.

Users must maintain the operational effectiveness ie keeping the batteries charged when required to be contacted.

Devices that have the ability to be password protected must have this security feature activated at all times.

International and premium number call facilities must not be used.

Users are prohibited from using mobile devices while operating a motor vehicle in the conduct of CHNC business.

Users must report any loss or theft, damage or security breach immediately. If such loss, theft or damage us due to the negligence of the user, the user maybe responsible for the cost of replacement or repair.

4 Monitoring, email, files, internet downloads or data storage

CHNC reserves the right to access and monitor any computer or other electronic device connected to the network. Access and monitoring of equipment is permitted for any reason, including but not limited to suspected breaches of this policy by a user or unlawful activities.

5 Breach of this policy

Where CHNC suspects or finds evidence of a breach of this policy, they reserve the right to restrict the users access to its IT resources.

Any user found to have violated this policy may be subject to disciplinary action.

Criminal offences will be reported to the police.