Information Technology Policy

1. Purpose

Inala Community House (ICH) recognises that its information technology resources are critical tools supporting the efficient and effective delivery of services to its clients.

ICH also acknowledges that there are a number of serious risks or consequences that may affect ICH, its employees and its clients if these resources are used inappropriately or are vulnerable to unauthorised access or disclosure.

2. Scope

This policy applies to all users who access or use any computer or other electronic devices (including laptops, tablets and mobile phones) whether owned, leased or used in order to access ICH technology resources including email, databases or ICH owned accounts on external servers, computers or other systems.

This policy shall apply to all staff, Board Members, contractors, students, volunteers or any other person who is undertaking any task on behalf of ICH. For the purpose of this policy, these persons shall be referred to as workers.

3. Definitions

Approved Devices means a worker's personal device which has been approved for ICH work-related use.

Devices include laptops, tablets, phones, hard drives, USBs or any other device which can either store, share or transmit information.

Data includes all information which belongs to ICH which may be stored on data storage devices, on a server, through work email accounts or online databases. For the purposes of this policy, this does not include ICH information which is available to the public (i.e. Facebook, ICH website, etc.).

Information Technology is a broad term used to describe the use of systems which access, store or send information and the equipment used to facilitate this.

Confidential Information in this context is determined by the ICH Confidentiality policy. For clarification, confidential information does not include: information generally available in the public domain or that was known by the worker prior to the disclosure by the organisation, its employees, representatives or associates.

4. Policy

ICH shall take all reasonable measures to ensure the integrity of its information technology resources and to protect confidential information stored therein. ICH workers must maintain these standards in their use of IT resources and shall at all times comply with all policies, procedures and directions from the Chief Executive Officer or Managers as business needs dictate, especially with respect to:

- the privacy and confidentiality of information;
- the use of technology for the business of ICH;
- the access to databases not developed, owned or operated by ICH.

4.1 ICH Data Storage

ICH stores information in a variety of different ways in order to provide efficient services and to comply with data storage requirements. ICH uses local servers and online databases (such as Sharepoint) to store information. These data storage systems are located within Australia and workers must be authorised to access them. In order to ensure the usefulness of data storage systems, workers should use appropriate naming protocols and file information in appropriate locations.

ICH uses multi-factor authentication wherever possible including Microsoft products and accounting packages.

4.2 Devices

ICH may provide workers with devices as required for work related purposes. These devices may also be approved to be taken offsite subject to any requirements (such as completion of a sign out agreement).

All devices containing confidential information (or with access to confidential networks) must be secured with either a PIN, password or encrypted in order to protect confidential information that may be stored. If a device containing confidential information is lost, the worker must immediately report this to their Manager or the Chief Executive Officer.

Use of Personal Devices for Work Purposes

Access to ICH data using personal devices is not permitted, except where authorised by policy, procedure or by a Manager. Where authorised, these may be considered as approved devices and therefore may be subject to provisions within this policy. Approved devices should be used in compliance with this policy and should not be used inappropriately for work-related purposes. Where approval is granted, the worker must take all reasonable precautions and directions from the Manager or Chief Executive Officer to protect any confidential information accessed. Workers should be aware that all ICH data remains the property of ICH, regardless of whether it is stored on a personal device.

Personal Phone Use

ICH understands that workers have a variety of responsibilities or obligations which may require them to use their phone during work hours. Workers are permitted to make personal calls on a limited basis (subject to the same limitations as personal use of internet in section 4.3).

4.3 Internet

ICH recognises that access to the internet is a crucial resource in the efficient performance of services. However, there are also substantial risks associated with this resource such as malicious software and possible confidentiality breaches. Workers should carefully consider the websites that are accessed, and any files downloaded in order to safeguard ICH IT resources.

ICH internet can be used for any work-related purposes. It must not be used inappropriately (as stated in section 4.5 below).

Workers may use the internet for limited personal use where it:

- Is infrequent and brief;
- Does not interfere with the worker's duties or the operations of ICH;
- Does not interfere with ICH security, storage capacity or network performance;
- Does not create additional expenses for ICH;
- Does not violate laws, privacy or confidentiality requirements.

Reasonable acceptable use of internet may include: paying a bill, sending a brief personal email, etc. Workers should take into consideration that ICH devices, internet and email may be monitored (see section 4.6 below).

4.4 Emails

ICH emails can only be accessed using issued or approved devices in order to protect the confidentiality of all clients, workers and operational information. Workers shall not access ICH email on any other device (whether owned by an employee, any other person or any other organisation or entity) except where authorised by policy, procedure or by a Manager or the Chief Executive Officer.

Internal ICH email containing organisational, service or client information cannot be forwarded or copied to personal email accounts, or persons and organisations unrelated to service clients or funders unless authorised by the relevant Manager, or the Chief Executive Officer. Forwarding or copying of email must be due to a genuine business need as confidentiality is paramount. This does not apply to the forwarding of payslips or other personal files (such as a worker's own employment agreement).

4.5 Inappropriate Use

Inappropriate use of Information Technology includes:

General

A worker shall not transmit unsolicited communication relating to:

- Solicitation of causes unrelated to the business of ICH unless officially sponsored or sanctioned by the Chief Executive Officer;
- Chain letters or texts

Security

A worker shall not create a breach of security or disruption of services whether targeted at ICH or outside the organisation through:

- Circumvention of any security protocols or programs or intentionally compromising the network through the introduction of malicious code which may include: viruses, worms, Trojan horses, email bombs, spyware, adware and keyloggers;
- Any use which cause any disruption to the network services through ICMP floods, packet spoofing, denial of service, heap or buffer overflows and forged routing information;
- The use of IT for unlawful activities, such as hacking in order to gain access to an unauthorised computer or network.

Workers should be careful when clicking unknown links or attachments as these pose a security risk.

Confidentiality and Privacy

A worker shall not use IT which results in a breach confidentiality or privacy requirements, such as:

- Sending, without permission, internal or confidential communications to another organisation or person which could benefit from the information;
- Posting images of ICH clients, events or activities on any social media site, website, or sent to a person or other organisation outside of ICH without the written approval of the Chief Executive Officer.

Offensive Material

A worker shall not access, view, display, download, store, transmit, share, print or otherwise use, distribute or solicit information, language or graphics which are considered offensive. This includes:

- The use of abusive, degrading, bullying or other offensive language or graphics;

- Racist, pornographic, criminal, obscene, abusive, culturally insensitive or inappropriate, degrading, bullying or otherwise offensive material;
- Sexual comments or images;
- Any comments that might offend someone due to their age, gender, sexual orientation, religious or political beliefs, national origin or disability;
- Messages which have the potential to be viewed as defamatory, threatening or obscene.

Copyright

The uploading or downloading of software, games, music, pictures, movies in violation of copyright laws is not permitted.

Workers may not use ICH information technology resources to play games during work time.

4.6 Privacy and Monitoring

ICH reserves the right to monitor IT, email and internet use in order to maintain the standards outlined in this policy, to ensure the security of technology and the confidentiality of information or to conduct maintenance of the system.

All ICH devices or IT systems and the data stored on them are and remain the property of ICH. This includes all forms of communication composed, sent and/or received. Workers should understand that any data which is stored on ICH devices can be accessed by the Chief Executive Officer or a designated worker.

ICH may conduct forensic computer examinations randomly, and in the event of a suspected breach of policy, whether by a worker or as a result of an attempted or successful external access to its technology and systems. Monitoring by ICH may take place on a continuous and ongoing basis.

4.7 Standards of Communication

Workers should ensure that the form and content of any communication sent on behalf of ICH or any of its services or programs is drafted in a professional and appropriate manner. Depending on its content, an email or message may constitute a formal business record. If this is the case, the worker who sends or receives the email or message must ensure that it is stored in compliance with all policies and procedures on the retention of business records.

Any communication must not be transmitted where it contains inappropriate information, images or graphics (in accordance with 4.5).

4.8 Remote Access

Remote access is a function which involves allowing access to a device by another party, including access to the ICH network. This is a valuable tool which allows IT support to

diagnose or remedy device or software issues, however this also poses a risk to the security and integrity of information held by ICH. Workers must not give remote access to ICH devices without prior authorisation from the Chief Executive Officer or Manager.

4.9 Breach

A breach of this policy may result in disciplinary proceedings up to, and including the termination of employment or dismissal from ICH.

In cases where the organisation has incurred costs due to a worker's breach of this policy, Inala Community House may seek to recover such costs from the worker.

4.10 Reporting Breaches

Any worker who becomes aware of a possible breach of IT security (for example, suspects a virus on an ICH computer) must report this to the IT department by emailing techsupport@ich.org.au. Any potential, suspected or actual breach of confidentiality should be reported to the Chief Executive Officer. The Chief Executive Officer shall determine whether this is a notifiable data breach (in accordance with the ICH Privacy Policy).

5. Review

This policy shall be reviewed every 2 years.

This policy remains in effect unless otherwise determined by resolution of the Board of Directors.

6. Related Documents

Policies

ICH Code of Conduct Policy
ICH Confidentiality Policy
ICH Privacy Policy
ICH Social Media Policy

Forms

ICH Laptop Sign Out Agreement
ICH Phone Sign Out Agreement