

Goondiwindi SILO Inc t/a Gateway To Training



GTT Cyber Safety Policy

Introduction

GTT is committed to maintaining a safe physical and emotional environment for all employees and clients. While acknowledging that the Internet and Information Communication Technologies (ICT) brings significant benefits to GTT's training programs and practices, the presence of these technologies raises a number of related cyber safety issues for the organisation.

Purpose

The aim of this policy is to maximise the benefits of ICT, while at the same time minimising and managing the risks. GTT acknowledges the need to have in place rigorous and effective cyber safety practices which are directed and guided by this policy.

Policy

GTT will develop and maintain rigorous and effective cyber safety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to learning and to the effective operation of GTT while minimising and managing any risks.

These cyber safety practices will aim to maintain a cyber safe environment as well as address the needs of clients to receive education about the safe and responsible use of current and developing information and communication technologies.

Definitions

The meaning of terms used in this document is:

- **ICT** - Information and Communication Technologies
- **Cyber Safety** - the safe and responsible use of the internet and ICT equipment and devices including mobile phones
- **Cyber Bullying** – direct verbal or indirect bullying behaviours using digital technologies including harassment via a mobile phone and/or social media sites; setting up a defamatory personal website, social media site and/or campaign; or deliberately excluding someone from social networking spaces
- **GTT ICT** - GTT's computer network, Internet access facilities, computers, and other ICT equipment and devices as outlined below
- **ICT Equipment and Devices** - includes but is not limited to computers (desktops, laptops, iPads, personal digital assistants -PDAs); storage devices (hard drives, solid state drives, USB and flash memory devices, CDs, DVDs, SD cards, floppy disks, tapes, and cloud storage), cameras (video, digital, webcams), all types of mobile phones, video and audio players and receivers (portable CD and DVD players), gaming consoles, and any other similar technologies as they come into use

Procedures

Cyber Safety Agreements

- No individual may use GTT's internet facilities and ICT devices and equipment in any circumstances unless the **GTT Acceptable Use of ICT Agreement** has been signed and returned

Note that User Agreements also apply to the use of privately-owned or leased ICT devices and equipment at GTT sites, or at or for any GTT related activity, regardless of its location, including off-site access to the GTT network from GTT or privately-owned or leased equipment

- GTT User Agreements will cover all clients and any other individuals authorised to make use of GTT's internet facilities and ICT devices and equipment where not subject to GTT's Acceptable Use of Computers, Internet and Email Policy.
- The User Agreements are also an educative tool and may be used as a preliminary discussion point for education purposes.
- Signed User Agreements will be filed in a secure place and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the internet and ICT devices and equipment
- Issues relating to confidentiality, such as sighting client or staff information, reasons for collecting data and the secure storage of personal details and information (including images) are subject to GTT's Privacy Policy

Appropriate Use of ICT

- All GTT clients and staff must abide by the organisation's internal policies and procedures including its Information Security Policy
- All users of GTT's ICT equipment and devices must comply with all legal requirements including anti-cyber bullying legislation, copyright and licensing agreements users who infringe these requirements will be personally liable
- Use of the internet and the ICT devices and equipment is to be limited to educational, professional development and limited personal usage which is both reasonable and appropriate to GTT's environment, as defined in the User Agreements
- The use of privately owned ICT equipment and devices at GTT sites or at any GTT related activities must be appropriate to GTT's environment – this includes any images or material present or stored on privately owned ICT equipment and devices (including mobile phones) brought onto GTT facilities or to any GTT related activity
- While GTT takes all reasonable precautions to screen material being accessed through information systems such as the internet, it may not always be possible for GTT to filter all material – it is the responsibility of all GTT staff and clients to immediately report any inappropriate content accessed on GTT's ICT

Monitoring

- GTT has the right to monitor, access and review all use of its ICT devices and equipment including personal emails sent and received on its computer/s and/or network facilities at all times
- GTT has the right to audit at any time any material on equipment that is owned or leased by GTT and may also request permission to audit privately owned ICT devices and equipment used at its sites and/or for any GTT related activity
- Where deemed necessary, stored content will be deleted and where possible and appropriate, staff and clients will be notified prior to this taking place

Breaches of GTT's Cyber Safety Policy and Procedures

The safety of GTT staff and clients is of paramount concern and any apparent breach of cyber safety including cyber bullying will be taken seriously.

- Any incident involving the unintentional or deliberate accessing of inappropriate material by staff or clients will be recorded
- In the event of access to such material, users should:
 - Not show others;
 - Close or minimise the window; and
 - Report the incident as soon as practical to their supervisor
- If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, the incident must be reported immediately to GTT's Executive Officer or a member of GTT's leadership team

The response to individual incidents will follow the procedures developed as part of the GTT's cyber safety practices, including:

- In serious incidents, advice will be sought from an appropriate source, such as the Office of the Children's eSafety Commissioner and/or a lawyer with specialist knowledge in this area
- There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases
- If illegal material or activities is suspected, the matter may need to be reported to the relevant law enforcement agency

Cyber Bullying

- GTT procedures dealing with cyber bullying are comprehensively set out in its Bullying Policy
- As this behaviour may constitute criminal misconduct, in such situations it may be necessary to involve law enforcement in addition to any disciplinary response made by GTT