Title	**Computer Systems, Internet, Email and Smart Phones Policy**
Document Type	**POL - Policy**
Document Owner	**Vince Stackpole**
Directorate	**DTI - Digital Transformation and ICT**
Date of Publication	9/09/2025 **Document Number** **IT-POL-0003**

1 Purpose

Communicare recognises that employees' need access to email systems and the internet to assist in the efficient and professional delivery of services. The purpose of this Computer Systems, Internet, Email and Smart Phones Policy is to provide guidance on the appropriate use of email, internet and Communicare's Information and Communications Technology (ICT) systems.

2 Scope

This policy applies to Communicare employees. This policy also applies to contractors, sub-contractors, consultants, volunteers and students as applicable.

3 Policy

Employees may be provided with ICT equipment to assist in the performance of their administrative, research and business activities. ICT equipment includes all computers, laptops/notebooks (e.g. netbooks and iPads), Printers, Smartphones (e.g. iPhone or Android phone) and other transportable computing and electronic devices, wireless devices, software, hardware, services, communications, and data including the Communicare Intranet.

All ICT equipment remains the property of Communicare.

3.1 Personal use

Personal use of Communicare ICT Equipment is permitted where it is brief and does not interfere with the duties of the employee, the employee's colleagues, the operations of Communicare and does not compromise the security of Communicare's ICT systems.

Employees may not use, divert or take Communicare property, equipment, services or assets for personal benefit such as the employee's personal business.

Although Communicare respects the individual privacy of its employees, that privacy does not extend to work-related matters and use of Communicare's e-mail and ICT equipment. Employees should not use ICT equipment for any communications which they wish to keep private.

Communicare cannot be held liable for any loss, transfer or publication etc. of any data that employees store on Communicare's ICT equipment.

Communicare reserves the right to determine the extent and nature of personal use of its e-mail and computer systems and may withdraw this privilege at any time.

Personal use of Communicare ICT equipment should be done responsibly and in accordance with this policy.

3.2 Monitoring and surveillance of Communicare systems

Employees should be aware that Communicare monitors its ICT equipment to ensure secure and efficient maintenance of our system and to identify and manage unacceptable standards of conduct by employees. Communicare reserves the right to monitor and access (recover, read, copy or delete) any email or other communication made through ICT equipment including documents stored by you on any company computer. Access to the Internet is logged and monitored. Even after an electronic communication/file is deleted or an Internet session is closed, it is possible to recover or recreate that electronic communication, file or Internet session.

Under no circumstances is an employee of Communicare authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Communicare owned resources.

3.3 Prohibited use of email and ICT system resources

The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of prohibited use.

The following activities are strictly prohibited and could result in disciplinary action up to and including dismissal:

Email and communications

- Speaking or writing to an internet message board about company personnel, activities, business practices, programs, release schedules, policies, customers or any other matter relating to Communicare in breach of this policy or without authorisation:
    - Examples of prohibited behaviour could include posting information about work colleagues, discussing the merits of upcoming or released programs, offering personal opinions about organisation policies or decisions, or soliciting the opinions of others.
- Employees are not permitted to comment publicly, anonymously or otherwise, regarding Communicare confidential information.
- Creating, sending, on forwarding, archiving, storing, onsite or on a cloud service or similar, or distributing material which is discriminatory, violent, unethical, defamatory or offensive whether to other users internal or external to Communicare.
- Accessing, creating, sending, on forwarding, archiving, storing, onsite or on a cloud service or similar, or distributing any pornographic or sexual material to employees or other persons outside of Communicare.
- Accessing the web, creating, sending, on forwarding, archiving, storing, onsite or on a cloud service or similar, or distributing any obscene, offensive, indecent, or vulgar material to employees or other persons outside of Communicare.
- The misuse of social media as described in the Social Media Policy.
- Sending any Communicare proprietary or confidential materials to unauthorised persons.
- Soliciting outside business ventures, advertising for personal enterprises, soliciting for non-organisation related purposes, on-line trading or gambling within working hours except as authorised by management.
- Mass mailing of non-business messages to groups or individuals.
- Illegal or unethical activities that could adversely affect or damage Communicare's reputation.
- Sending or on forwarding copyrighted materials in violation of copyright laws or license agreements.
- Sending, forwarding or downloading copyrighted software or data, except where it is part of an employee's job description or authorised by management.

- Intentionally or deliberately propagating any malware, virus, worm, Trojan horse or trap-door program code.
- Attempting to disable, defeat or circumvent any organisation security tool, such as internet firewalls or encryption.
- Attempting unauthorised access to resources.
- Playing electronic games on the ICT equipment.
- Downloading music and video files and distributing them.
- Accessing any part of a database or system using another employee's login details without their express permission.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, chat, telephone, messaging or SMS, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or "pyramid" schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of social media newsgroups

ICT systems

The following activities are strictly prohibited on Communicare's ICT network and systems, with no exceptions:

- Violations of the rights of any person or organisation protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Communicare.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Communicare or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Communicare should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g. malware, viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your computer or account by others. This includes clients, family and other household members and is effective whether the computer is being used at a Communicare facility, off-site or while working from home.
- Using a Communicare computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any Communicare account.
- Making statements about warranty or guarantees on behalf of Communicare, expressly or implied, unless it is part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless

these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless approved by management.
- Executing any form of network monitoring which will intercept data not intended for the employee's host PC, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host (PC or Server), network or account.
- Interfering with or denying service to any user other than the employee's host PC (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Communicare employees, Communicare clients and Communicare business partners to external parties.
- Installing games, non-business Instant Messaging software (e.g. Yahoo Messenger, IRC etc.), unauthorised multi-media programs, social networking sites (e.g. Facebook, Twitter) devices (personal video cameras, personal entertainment devices, non-compatible personal printers etc.).

3.4 Bring Your Own Device (BYOD)

The use of personal mobile devices (iOS or Android) is permitted while accessing Communicare resources provided Microsoft Company Portal is installed on that device and logged in with Communicare credentials. Devices attempting to access Communicare resources without Microsoft Company Portal will be actively blocked.
Desktop or laptop computer devices (Windows, or MacOS) can access Communicare resources but only within browser provided instances of Microsoft 365.

Use of a BYOD is entirely at the risk of the owner – any costs or damage associated will not be the responsibilty of Communicare.

If a personal mobile device (ios or Android) which has access to Communicare Devices is to be taken overseas, the Microsoft Account must be logged out and corporate applications deleted.

3.5 Courtesy

The use of abusive, vulgar, or objectionable language on the Internet or ICT equipment is unacceptable. Additionally, using the Internet for the intentional harassment or harm of an individual or organisation is prohibited.

3.6 Lawfulness

It is not acceptable to use Communicare's networking services, ICT equipment, resources or facilities for any purposes that violate existing state, or federal laws or international laws, regulations, policies or procedures. Illegal usage will become the responsibility of the user and will lead to disciplinary actions against the employee.

3.7 Failure to Follow Internet Usage This Policy

Communicare retains the right to monitor employee activities; Communicare's ICT Team will monitor and audit Internet access and ICT equipment for the purposes of assuring system security, proper usage, and for performance impact. The employee has no rights of privacy in their use of the Internet or ICT equipment when using company property.

3.8 Reporting inappropriate use of ICT equipment

The following processes should be followed to report inappropriate use of the email, communications or the system and network:

1. If an email is received by an employee which contains inappropriate content, the employee shall immediately reply to the sender asking them not to send such content.
2. A copy of the reply should be sent to the employee's relevant Manager or Director. The email should then be deleted.
3. Any other form of receipt of inappropriate material (including by text message) should also be brought to the attention of the employee's relevant Manager or Director.
4. If an employee becomes aware of another employee's inappropriate use of email, communications or system or network, the employee's relevant Manager or Director should be informed.

3.9 Leaving Communicare

Upon termination of employment, employees are not permitted to delete any data, including personal information and emails, from Communicare computer equipment or computer systems.

3.10 Disciplinary action

Disciplinary action up to and including termination of employment or services may result from any breach of this policy. Other actions that may result from a breach of this policy include:

- Loss of internet access; and
- Exposure to civil or criminal liability.

4 Responsibilities

All Employees are responsible for being aware of and adhering to this policy.

5 Abbreviations, Acronyms and Definitions

BYOD	Bring Your Own Device
HR	Human Resources
ICT	Information and Communication Technology
ICT equipment	ICT equipment includes all computers, laptops/notebooks (e.g. netbooks and iPads), Personal Digital Assistants (PDAs), Smartphones (e.g. iPhones) and other transportable computing and electronic devices, wireless devices, software, hardware, services, communications, and data including the Intranet.
Intranet	An intranet is a computer network that uses internet protocol technology to share information, operational systems, or computing services within an organisation.
PC	Personal Computer
SMS	Short Messaging Service
WAN	Wide Area Network

6 Related Documents

Computer Equipment Policy
Confidentiality Policy
Security Policy
Social Media Policy
Termination Policy
Sexual Harassment Policy
Workplace Bullying Policy
Responding to FDV in the Workplace

7 Document Governance

Prepared by:	Sheydn Rowe	Business Analyst	12/5/2021
Approved for use by:	Melissa Perry	CEO	9/09/2025
Second Approver (if required)			
Date endorsed by the Board (only applicable to certain policies):			
Summary of change from last revision (n/a if first time issued):	n/a		