INTEGRITY COMMISSION TASMANIA

Information and communication technologies

The use of information and communication technologies is a major misconduct risk area, so it is important to understand your responsibilities in relation to using them.

What are information and communication technologies?

Information and Communication Technologies (ICT or ICTs) refers to all communication technologies that enable users to access, retrieve, store, transmit, and manipulate information in a digital form.

Examples of ICTs in the workplace are:

- desktop and mobile computers, including cameras, speakers and other devices
- mobile phone
- information management software systems (such as Microsoft Outlook) that allow you to send and receive emails, use a calendar, manage tasks, manage contacts, take notes, log journals, and browse the web
- customer, client or patient record management systems
- network, server, storage and cloud resources
- databases and mailing lists
- receipting and licence/permit documenting systems
- video-conferencing hardware, and
- social media applications, including websites.

Most public sector employees are provided with ICT resources and services to perform their duties. ICT resources include tangible resources (phones and computers) and intangible resources (internet service and software applications).

Built into ICT systems are security measures that include network protections, prevention of data breaches and secure data storage for data privacy, protection and compliance.

These ICT systems and security measures rely on employees using them with integrity and complying with their relevant codes of conduct.

Using ICT with integrity

As a public sector employee, you have been placed in a position of trust. Your role may include having access to personal information and records.

Appropriate use of ICT is an essential component of public service. Always follow policies and procedures, and don't exceed your authority to access and manage data. If you are not sure, ask your manager.

ICT misuse

Most ICT misuse falls into three categories:

- theft of hardware and software
- unauthorised access to computer systems, and
- inappropriate use of equipment.

Examples of ICT misuse are:

- using a work computer to search the internet for personal reasons
- using a work computer to access inappropriate material, such as pornography
- using a work phone to place bets
- copying information without authorisation, such as information about forthcoming announcements or events
- manipulating a computerised accounting or payroll system
- accessing information without authorisation
- accessing information when it is inappropriate to access, such as information about a friend or neighbour
- sending emails or social media messages to a colleague to harass or bully them, and
- inserting a malicious code or interfering with computer networks.

Outcomes of misuse

The outcomes of misuse can damage your organisation and public confidence. It can also lead to disciplinary measures against you, such as sanctions, warnings, penalties or reassignment. Serious misconduct may result in dismissal and/or criminal investigation.

ICT fraud

Theft of telecommunications or computer equipment (including mobile phones) is a costly form of misconduct for many public sector organisations.

The value of computer equipment is more significant than just the replacement cost of the hardware. A particular example is when the device has been used to store copyrighted, sensitive or customer-related data.

The procurement of ICTs is another misconduct risk area, with opportunities for corruption, fraud and contract mismanagement.

Inappropriate access to personal information

There are significant implications of misuse of ICT in the public sector, mainly owing to the amount of data held by public sector organisations.

Public-held data includes:

- health, income, employment and education information
- details about contact with the criminal justice system
- personal information such as address and date of birth, and
- photographs associated with licences and passports.

You may also have access to data that could track individuals' movements and daily activities, such as public transport usage.

Unauthorised access is a significant contributor to data breaches, as employees may use legitimate access to computer systems in inappropriate and unauthorised ways.

CASE STUDY

Over a three month period, a Centrelink employee created 26 Centrelink customer accounts in false names and had benefits paid to those accounts. He then obtained the benefits for himself.

The defendant also had payments in the form of Electronic Benefit Transfers made to four accounts of Centrelink customers known to him without their authorisation. He then obtained the money for himself.

The defendant fraudulently obtained a total amount of $66,120.36 and was charged with 30 counts of obtaining property by deception. He was sentenced to a total sentence of four years imprisonment to be released after serving 18 months. In sentencing the defendant the Court stated:

"...in dealing with this sort of fraud, particularly where the person involved is a government employee, there is a significant need for the sentence to be such that it will deter others in a position of trust who are minded to attempt to defraud the welfare system."

With thanks to the Australian Institute of Criminology report[1]

Personal use

Generally, it is not appropriate for any public resource to be used for private gain.

However, subject to your organisation's policies, it is reasonable for employees to have limited private use of office equipment. For example, occasional or necessary telephone or email communication with family is usually acceptable.

Misuse of email

Email misuse includes sending emails and attachments that contravene an organisation's internal policies, such as codes of conduct, email usage, and sexual harassment policies.

If the email relates to disclosing a sensitive matter, your organisation may treat it as serious misconduct.

Your organisation may also refer the matter for criminal investigation if the misconduct is serious, for example, the possession or distribution of child exploitation material or emails that threaten, menace, harass or cause offence.

What to do if you are not sure or if you suspect misuse is taking place

Your organisation will have policies and procedures to guide you in making good decisions about using and managing information and communication technologies. Speak to your manager if you are unsure.

[1] https://www.aic.gov.au/sites/default/files/2020-05/tandi470.pdf

- **The Commission can help**
- We are available to provide support and assistance with identifying, reporting, investigating, managing and preventing misconduct: prevention@integrity.tas.gov.au or 1300 720 289.
- For more Misconduct Prevention resources go to www.integrity.tas.gov.au/resources