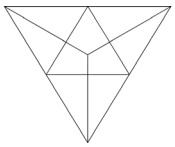
WORK INFORMATION



INTEGRITY COMMISSION TASMANIA

Using work information with integrity

You have a legal requirement to protect all work information about government business, staff, clients and customers.

Work information in the public sector

Work information is data, information, or content generated, collected, or funded by the government or public organisations.

Work information can come in a variety of forms, including:

- physical and electronic records of documents, files, letters, emails, recordings, images
- the contents of databases or spreadsheets, and
- the copyright and intellectual property contained in documents, plans or other media.

It can also be verbal – something you overhear or see at work, or perhaps a client tells you.

Handling work information appropriately

All public sector organisations should have in place policies, protocols and procedures for the appropriate handling and security of work information.

Your organisation should provide you with the relevant policies and procedures for your role – you must comply with and follow them at all times.

If you are an employee of the state public service, the Code of Conduct ('the Code') is part of the *State Service Act 2000* (Tas)[1] and is part of your employment framework. Compliance with it is a condition of your employment.

The Code includes specific references to work information:

(7) An employee must maintain appropriate confidentiality about dealings of, and information acquired by, the employee in the course of that employee's State Service employment.

(9) An employee must use Tasmanian Government resources in a proper manner.

(11) An employee must not make improper use of –

(a) information gained in the course of his or her employment; or
(b) the employee's duties, status, power or authority –

in order to gain, or seek to gain, a gift, benefit or advantage for the employee or for any other person.

Other legal requirements

Other acts refer to the proper use of work information. For example, under the *Integrity Commission Act 2009* (Tas)[2] , it is misconduct for a public officer to misuse information or material acquired in, or in connection with, the performance of the public officer's functions or exercise of the public officer's powers.

Balancing transparency and privacy

The public's right to information

Open and transparent government is in the public interest and is key to promoting integrity and accountability in the public sector. According to legislation, information in the government's possession or under the government's control is a public resource.

Openness in government increases the participation of members of the community in democratic processes, leading to better-informed decision making.

Therefore, the public must have the right of reasonable access to information in the government's possession or under its control **unless**, on balance, it is contrary to the public interest to provide that information.

Personal information protection

Public sector organisations collect and store a large amount of information about staff, clients, patients and customers.

They are required to protect the privacy of individuals by controlling the ways in which they collect, keep, use, and release records containing sensitive personal information that clearly identifies an individual.

Balancing transparency and privacy can be challenging. Make sure you follow the policies and procedures for your role at all times and seek advice if needed.

Abuse of work information

Abuse of work information occurs whenever information is accessed, shared, altered or created for any purpose other than to perform your work duties. It can violate the public's trust, place citizens in uncomfortable and dangerous situations, and jeopardise government security.

Reckless or negligent conduct that results in the release of work information may lead to disciplinary action against the responsible employee.

Deliberate abuse of work information is treated seriously. In addition to contravening the State Service Code of Conduct, it may be an offence under the *Criminal Code 1924* (Tas)[3] and *Police Offences Act 1935* (Tas)[4].

CASE STUDY

In 2012, the boyfriend of an employee of Queensland Department of Transport and Main Roads (DTMR) reported that his now ex-girlfriend was accessing DTMR records and providing addresses and other information to third parties.

Following a joint investigation, the employee was charged with 94 criminal offences, including 88 separate counts of official corruption.

The court found the employee fraudulently issued or transferred 31 vehicle registrations and issued or upgraded 57 driver licences, and received at least $20,000 in cash for the fraudulent transactions.

She was sentenced to four years imprisonment to serve six months, after which the sentence was suspended for four years, for fraudulently issuing driver licences, licence upgrades and vehicle registrations in return for cash payments.

Extracted from Operation Impala report, QLD CCC[5]

High-risk information

The increasing use of electronic systems to collect, transfer and store information, and their vulnerability to internal misuse or external attack, is a significant risk.

High-risk work information includes:

- information classified by policy or legislation as sensitive, confidential or protected
- identity and other personal or financial information (including commercial-in-confidence material), privileged, proprietary or business information
- in-confidence material, and
- information that may cause harm or give an unfair advantage if lost, damaged or released without authorisation.

Common types of information abuse

Abuse of work information most commonly occurs through:

- unauthorised access
- breach of confidentiality or protection

- use of information for personal gain
- use of information to bully, harass or prey on others
- inappropriate creation or alteration of information
- failure to protect sensitive information, or
- inappropriate use of social media.

Separate fact sheets on each of these topics are available on our website.

How to prevent abuse of work information

Before you access work information, ask yourself:

- Am I accessing this information to perform my work duties?
- Am I sharing this information with someone authorised to access and use it?
- Am I sharing this information for a work-related purpose?
- Have I taken all necessary precautions to ensure this information is protected?
- Am I creating or altering this information as part of my work duties?

If you answer **no** to any of these questions, you may be abusing work information.

If you still feel uncertain, seek advice from your manager about handling information appropriately in your circumstances.

Adapted with permission from Queensland CCC Corruption Prevention Advisory – information security and handling 2016[6]

---

[1] www.legislation.tas.gov.au/view/html/inforce/current/act-2000-085

[2] www.legislation.tas.gov.au/view/html/inforce/current/act-2009-067

[3] www.legislation.tas.gov.au/view/html/inforce/current/act-1924-069

[4] www.legislation.tas.gov.au/view/html/inforce/current/act-1935-044

[5] www.ccc.qld.gov.au/publications/operation-impala-report-misuse-confidential-information-queensland-public-sector

[6] www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Corruption-Prevention-Advisory-Information-security-and-handling-2016.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