WORK INFORMATION

INTEGRITY COMMISSION TASMANIA

Frequently Asked Questions

1. What is work information?

Work information is any information you can access in your workplace or role. This primarily means information in your organisation's databases, electronic files and hardcopy documents. It also includes information you hear in the course of your work, read in emails, and information from internal sources, such as the staff intranet.

NOTE: work information is still protected even if that information is also accessible to you privately or is in the public domain.

2. Why is it essential that all work information be protected?

You need to protect all work information for a few reasons:

- it is not always clear whether a piece of information is important or sensitive
- information is collected for a reason and therefore serves a purpose in the running of government
- the government is trusted with this information and must treat the information with appropriate care and protection, and
- information is government property, so it must be protected and maintained like physical government property.

So, while some information may seem pointless, its release can cause harm to individuals and the government.

3. What are my legal and work duties concerning the use of information?

Your responsibilities and obligations are contained in a few different areas:

- your organisation's code of conduct – this will require that you only use information appropriately
- *Tasmanian Criminal Code* (sections 110 and 257D) requires that you not disclose official secrets or access a computer without authorisation. Both of these actions are considered criminal offences.
- *Police Offences Act* (section 43C): requires that you not access a computer without authorisation
- *Integrity Commission Act 2009* (section 4): defines misconduct as including misuse of information, and

- your employment contract: this may include a condition of employment that you use information appropriately.

  It may also include a confidentiality waiver or non-disclosure agreement requiring that you not disclose certain information or knowledge even after leaving the organisation. If you are unsure, check your contract.

As a public employee, you have many different professional and legal obligations to use information appropriately. The best course of action is to be diligent in its handling and use.

4. What should I do if I access information to perform my work duties, but that information coincidentally benefits me personally?

If you have accessed the information for a legitimate work purpose, you have not committed misconduct. However, you need to ensure that this coincidental benefit does not cause any future problems.

First, you should talk to a supervisor and make them aware of the incident, the benefit you have gained, and why you were accessing the information. They will record this incident to protect you from potential future misconduct allegations and take further appropriate steps.

Second, you should declare any conflict of interest to Human Resources. While it is unlikely that any further action will need to be taken, this will allow the conflict to be managed to minimise any misconduct risk.

5. Is misuse of information punished seriously?

The punishment for misuse of information is dependent on the seriousness of the misuse, the nature of the information and whether it has occurred before.

Misuse of information can be a criminal offence and can have serious consequences. Sanctions can include fines, re-assignment of duties, termination of employment and, in some cases, lead to criminal charges and convictions.

These outcomes are not uncommon and can occur in situations that do not appear serious, such as the WA police officer who looked himself up on a work database and received an $8,000 fine.

6. Do I still have obligations to avoid misusing information if I no longer work for the public sector?

Your capacity to misuse information will be greatly limited once you leave your public sector employment, as you will no longer be able to log into the database or access files. However, you may be aware of information that is confidential and protected by the organisation.

To understand your obligations, check your exit contract and any legal documents you signed to determine if you are still bound by confidentiality.

The best practice is to treat any information you have gained in your workplace as confidential and sensitive. This way, you uphold the duties you had when you became aware of this knowledge in the course of your work and will not violate any legal obligations.

7. Suppose a misuse of information enables more serious misconduct, such as bullying or theft. Will the offending person be punished for both acts of misconduct or only the more serious act?

The different code of conduct violations will be treated equally and just as seriously. Any alleged code of conduct violations are likely to be investigated and, if substantiated, the perpetrator punished.

8. Who should be the first person I talk to if I have questions about misusing information or I suspect others of misusing information?

If you have any concerns about the misuse of information, you should first approach your supervisor or manager. Your manager will be able to explain your organisation's policies and procedures concerning misconduct and will point you in the right direction.

Your second support will likely be the HR department, as they handle your organisation's code of conduct and will have more specialised knowledge about misconduct and reporting.

If you feel that the appropriate steps are not being taken internally or are worried about bringing this issue up within your organisation, you can seek external assistance.

The Integrity Commission has specialised knowledge and expertise on misconduct and has the capacity to both educate on misuse of information and conduct investigations into alleged misconduct.

9. Our systems are so old that it is easy to accidentally stumble across information you shouldn't and don't want to access. Is it misconduct if people are not intentionally accessing inappropriate information?

If you have accidentally stumbled across information by no fault of your own, you are not likely to be accused of misconduct.

The appropriate actions to take are to talk to a supervisor immediately and inform them of the incident. Once they are aware of the details of the incident, they can determine what steps should be taken.

In such a situation, it is good practice to report any systemic or technical faults to a manager or senior leader to minimise any future accidental breaches. Hopefully, the result would see the aging systems updated to prevent such accidents from occurring.

10. How can 'loss of data' be considered a misuse of information when I'm not using the data because I have lost it?

It may seem odd that a loss of data, where you are not using nor have access to information, can be considered a misuse of information. However, the misuse does not occur when it was lost but when the loss results from carelessness or negligence.

It may be treated as misconduct because loss of data can create the same level of harm as a breach of confidential information or inappropriate distribution of information.

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