

Integrity Spotlight

V1.1 – January 2023

Advisory Confidentiality and misuse of information

The misuse of information can undermine the proper functioning of government responsibilities, processes and programs.

Introduction

An agency's most valuable assets are its people and its information. However, the interaction of people and information carries significant risks of corruption and improper conduct.

To mitigate the risk of corruption, agencies must ensure appropriate controls are in place to protect sensitive information and public officers must understand and comply with all directions around the legitimate and appropriate use of information.

What are the risks?

The misuse of information can undermine the proper functioning of government responsibilities, processes and programs.

In many cases, inappropriate access of information is done out of mere curiosity, with no intention to disclose or misuse the information. Although this is unacceptable and breaches public trust, the more serious end of the spectrum can have significant consequences for individuals, businesses and agencies. For instance, when sensitive procurement information is improperly provided to favour a supplier, other businesses lose opportunities and money, and the agency forgoes the chance to achieve the best value for money.

The safety and security of individuals might also be at risk if personal details are disclosed in circumstances where domestic abuse or disputes are present, and the disclosure of medical records has the potential to cause substantial distress.

Sometimes information is misused for self-gain. For example, having prior knowledge of government decisions might determine whether or not you buy a house in a particular area. But it can also be the case that third parties might target public officers in an effort to gain access to information. Grooming, bribery and extortion of public officers for valuable information is often associated with criminals and organised crime groups. However, anyone with a motivation to profit from confidential information could seek to target public officers.

What types of information are at risk?

The types of information that are at risk include:

- Personal information such as names, addresses, phone numbers and financial information which could be used to engage in identity fraud
- Medical information
- Prisoner information, police holdings and criminal records
- Information related to recruitment (for example, interview questions)
- Information related to procurements and tenders (for example, competitor offerings, project budget, and evaluation methodology)
- Business, market-sensitive or proprietary information
- Information related to land value, land zoning, property and development decisions
- Commercial-in-confidence, or cabinet-in-confidence
- Information from closed or in-camera meetings
- Intellectual property
- Information protected or classified under legislation
- Information which could cause harm or disadvantage if released, lost or altered

Public authorities should be aware of the value of all information holdings, and the potential for that information to be misused.

Misconduct

Public officers who improperly access or use information should face disciplinary actions, and in serious cases such conduct may result in the public officer's dismissal.

Guidance on the use of official information for public sector employees is primarily provided by the Code of Ethics for the South Australian Public Sector, issued by the Commissioner for Public Sector Employment, which states:

Handling Official Information

By virtue of their duties, public sector employees frequently access, otherwise deal with, and/ or are aware of, information about issues, facts and circumstances that they know, or where a reasonable person in the circumstances would know, needs to be treated as confidential.

Public sector employees will not access or attempt to access official information other than in connection with the performance by them of their duties and/or as authorised.

Public sector employees will not disclose official information acquired through the course of their employment other than is required by law or where appropriately authorised in the agency concerned.

Public sector employees will not misuse information gained in their official capacity, including, but not limited to:

- *purchasing shares or other property on the basis of confidential information about the affairs of a business or of a proposed Government action; or*
- *seeking to use information for personal benefit or gain or for the personal benefit or gain of another.*

Public sector employees will maintain the integrity and security of official information for which they are responsible. Employees will also ensure that the privacy of individuals is maintained and will only release information in accordance with relevant legislation, industrial instruments, policy, or lawful and reasonable direction.

The handling of official information by local government employees and elected members is governed by the *Local Government Act 1999* and its instruments.

Criminal prosecution?

While it is clear that public officers improperly accessing, disseminating, altering or deleting agency information can lead to disciplinary action, including dismissal, it is not always understood that the consequences can extend to criminal prosecution.

Often the misuse or release of confidential information by public officers is for the purpose of facilitating other corrupt or dishonest schemes. Breaches of confidentiality should therefore be viewed as potential red flags for other criminal conduct.

Corruption related to the misuse of information may appear as:

- A public officer accessing confidential information in order to gain a personal benefit or advantage, or to improperly disadvantage, harass or intimidate another person.
- A public officer providing confidential information to others to assist them to gain a benefit or advantage, or to improperly disadvantage, harass or intimidate another person.
- A public officer misusing information for any purposes other than their official duties.
- A public officer accessing and retaining official information for some use outside their public role, or once they have left their public role.

However, in some egregious cases, a public officer improperly accessing work databases or misusing confidential information can expect to face criminal prosecution for that fact alone.

Case study

Correctional Officer prosecuted for using confidential government database like 'Google' and disseminating information to drug defendants

In 2022, a correctional officer pleaded guilty to multiple counts of abuse of public office and failing to act honestly in the performance of duties while working for the Department of Correctional Services in 2018 and 2019.

During that time, the officer had access to numerous internal sources of information, including the Justice Information System, a confidential government database containing information about offenders in South Australia's criminal justice system.

The officer worked as a home detention compliance officer and utilised access to the Justice Information System to alert a man on home detention about upcoming drug and alcohol tests. The officer also looked up the release date of a prisoner, as well as accessing and disclosing another man's address details for a friend. That friend was later charged and fined for counselling or procuring a public official to fail to act honestly in their duty. The officer also warned a colleague's daughter that a police taskforce was searching for her in a misguided attempt to "big-note himself".

The officer did not seek or receive financial benefit for disseminating the confidential information. Despite this, he displayed a cavalier attitude to the security of information in the Justice Information System, which threatened the integrity of processes such as home detention monitoring, criminal investigations and prisoner management. In using these information systems like 'Google', the officer was aware that "what he was doing was wrong", but admitted to not realising he was committing crimes by giving out the information he was improperly accessing.

The officer was sentenced to 12 months imprisonment.

What can agencies do?

To prevent the inappropriate access and misuse of confidential information, agencies should ensure the following:

Technology

- Ensure staff do not share their system login details, and eliminate or limit the number of systems which rely on shared logins.
- Systems holding confidential, sensitive or valuable information should have strong auditing capabilities to detect misuse, and auditing of those systems should occur on a sustained and targeted basis.
- Immediately remove system access from departing staff.
- Consider the use of login warnings or confidentiality notifications to systems when employees log on, or implement systems permitting access only after requiring users to first identify a purpose for their access.
- Limit or restrict access to highly sensitive information and determine system access only on a 'need to know' basis.




Staff

- Regularly communicate to staff policy expectations regarding the handling, storing, access and release of confidential information. Training which outlines the risks, impact and specified penalties for the improper access or unauthorised release of information should be repeated periodically. Training should foreshadow that information systems will be regularly audited to work as a deterrent for misuse.
- All employees should undergo induction training on policies, practices and procedures on information security and management.
- Remind staff with significant access to confidential information of conflict of interest policies which should mandate the declaration of personal or pecuniary interests which are likely to conflict (or could be perceived to conflict) with their official duties.
- Ensure that all staff exiting an agency have their access to information systems removed.

Policies and Procedures

- Create and maintain clear policies and procedures for the handling, storing, access and release of information.
- Create and maintain robust conflicts of interest and secondary employment policies.
- Ensure that agency procedures and practices accord with relevant information classification requirements.
- Agencies should implement comprehensive, proactive and ongoing audit regimes on key information systems.

CONTACT US

-  GENERAL ENQUIRIES
(08) 8463 5191
-  LEVEL 1, 55 CURRIE ST
ADELAIDE SA 5000
-  @ICAC_SA

ICAC.SA.GOV.AU



ICAC

Independent Commission
Against Corruption
SOUTH AUSTRALIA