Crime and Corruption Commission
QUEENSLAND

May 2016

Confidential information

Unauthorised access, disclosure and the risks of corruption in the Queensland public sector

Queensland's public sector agencies handle a variety of sensitive and confidential information. What may seem a simple "peek" by a public servant at someone else's personal data is not only an invasion of privacy, it's potentially a criminal offence and grounds for investigation by the Crime and Corruption Commission.

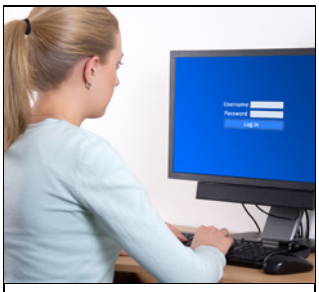
What are the corruption risks associated with access to and disclosure of confidential information? And how well are agencies learning the lessons from investigations of those complaints, to reduce the risks of such inappropriate access recurring?

Members of the public have every right to expect that their private information is not being accessed by or disclosed to anyone who does not have a legitimate reason to use it.

What you should know

- Directors-General and CEOs are accountable for the safe storage of confidential information held by government agencies and must ensure that this information is used only for lawful purposes.
- Under the law, improper use of information by public officers can be a criminal offence. It is a serious breach of the trust placed in every employee and the agency by the government and the public.
- Once information is released from an agency without proper authority, there is no guaranteed control over it. The agency cannot know who may come to possess it or what use they will put it to.
- Unauthorised access to confidential information by public officers is a significant and longstanding issue, and is one of the most common types of allegations and investigations that the CCC deals with.
- Since 1 July 2015 the CCC has finalised 15 investigations related to abuse of confidential information, resulting in 81 criminal charges and 11 disciplinary recommendations.
- A recent CCC audit revealed that some agencies were not regarding breaches of confidential information seriously enough, or properly understanding the risks involved.

The information contained in this paper is based on investigation outcomes, analysis of complaint data, and an audit of complaints relating to confidential information by Queensland public sector agencies.



Some agencies require any staff accessing their internal databases to declare that they are doing so solely for authorised purposes.

Confidential information and government agencies

Queensland public agencies collect and store a wide range of confidential and sensitive information that public officers access and use in carrying out the functions of the agency. Such information includes commercially sensitive information, residential and financial data, personal health records and criminal histories.

This information is held in trust for both the individuals concerned and the Queensland community generally. Community members have every right to expect that such information is not being accessed by or disclosed to anyone who does not have a legitimate and lawful reason to use it.

Improper use of confidential information occurs when an employee of a public sector agency accesses information held by the agency ***not*** to perform their normal lawful duties but rather for ***a private use and benefit,*** either for themselves or another person.

Potential criminal offences are spelled out in the Criminal Code, the *Police Service Administration Act 1990*, the *Information Privacy Act 2009* and the *Public Interest Disclosure Act 2010*.

Despite this, misuse of confidential information remains one of the most common types of corruption allegations referred to the CCC.

Confidential information is entrusted to an agency for identified lawful purposes, not for the personal use of its employees

Improperly accessed information included tendering and recruitment information, personal health data, criminal histories and custody information

Examples of inappropriate access or use of confidential information

Recent examples of allegations of the misuse of confidential information by public officers/employees that have been received by the CCC include:

- A procurement officer was alleged to be using his work email to forward quotes received from prospective contractors to another contractor (a friend), asking if the friend "can do any better".
- An officer, who was seeking to support a friend involved in court proceedings about a child, accessed confidential information about the friend's ex-partner's criminal history and other personal information through information systems only available to him through his work. His intention was to help the friend demonstrate the ex-partner's lack of suitability or capacity to care for the child.
- A senior officer involved in a recruitment process provided the interview questions to one of the applicants ahead of the interview. The applicant, who worked in the senior officer's team at the time, was ultimately successful in the recruitment process.
- An officer accessed confidential information related to the health of a family member and subsequently disclosed that information to another family member.

Once information is released from an agency without proper authority, there is no guaranteed control over it

Risks of improperly using confidential information

Improperly accessing and/or disclosing such information can:

- damage the reputation of the organisation or individuals
- provide unfair advantages (for example, commercial) to the recipients of the information
- adversely affect projects, activities and the public interest
- increase the likelihood of corruption (petty misuse is likely to lead to more systemic and serious abuse over time).

Once information is released from an agency without proper authority, there is no guaranteed control over it. Even if the original release was not intended to cause harm, the agency cannot know who may come to possess it or how they might use it.

Misuse of information and the Crime and Corruption Commission

The CCC is tasked with reducing the incidence of corrupt conduct in the Queensland public sector — especially the most serious and systemic — by receiving and investigating complaints and by keeping track of how agencies deal with corruption issues.

Investigation outcomes

Those cases in which access to information could constitute a criminal offence, or result in someone being dismissed from employment, are investigated by the CCC or the QPS. Since 1 July 2015 it has finalised 15 investigations related to abuse of confidential information, resulting in 81 criminal charges and 11 disciplinary recommendations.

The cases below show examples of penalties for public officers who accessed information without proper authority.

Case study

Criminal charges and convictions for information offences

A former Queensland police officer was sentenced to six months imprisonment (wholly suspended) for accessing and releasing confidential information to a relative who worked as a private investigator. The information included car registration details, addresses and criminal history records. His co-accused pleaded guilt to 14 counts of computer hacking and was given two and a half years probation.

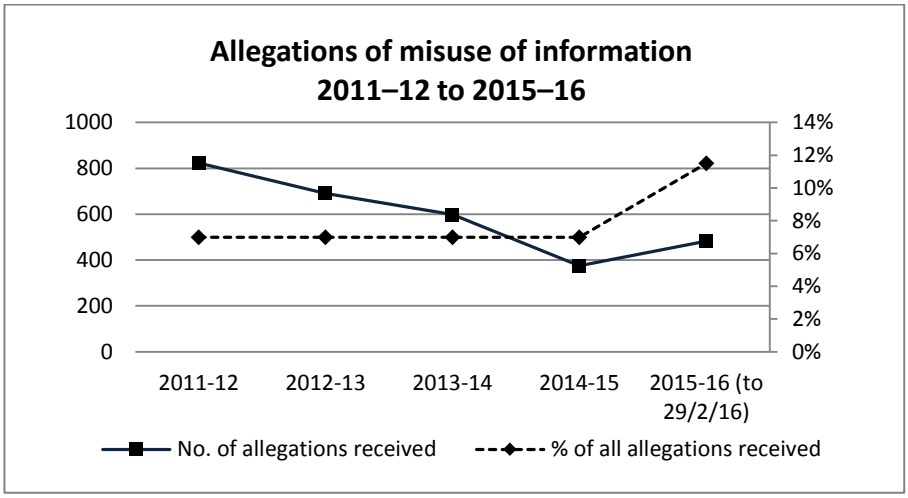
A police officer pleaded guilty to 50 offences of computer hacking. He was fined $8000 and had a conviction recorded. The officer had been regularly accessing various telephone dating services at work and then using the QPS database to access personal information about the individuals identified on the dating services.

A public servant was sentenced to 18 months imprisonment immediately suspended, with conviction recorded, for obtaining details from her employer's database about a client's property valuation and building inspection reports to inform decisions she and her husband were making about their personal property purchases. She had no work-related reason to access the information and had therefore gained an improper advantage. This conduct was aggravated by her deliberate concealment of her access to the records.

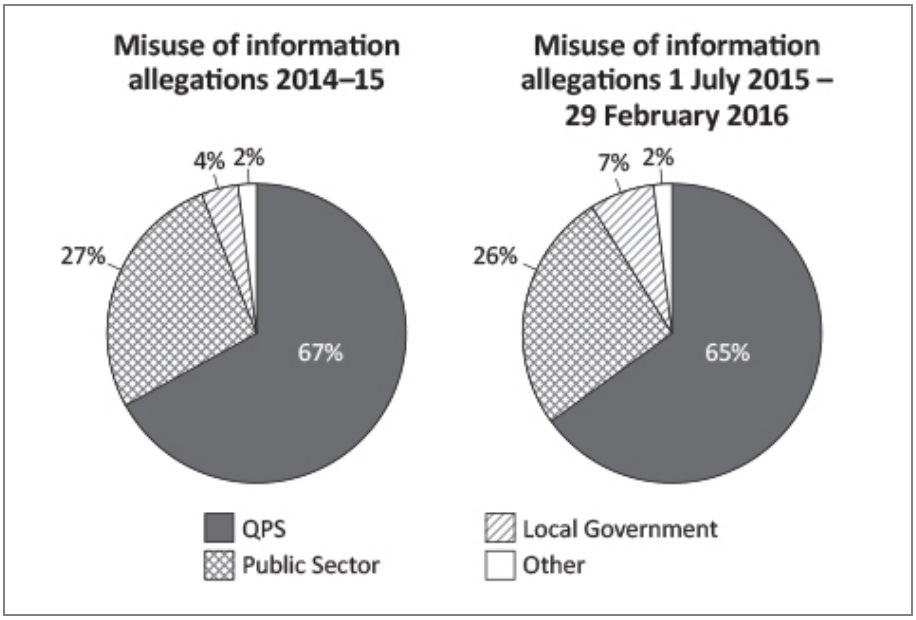
Complaints about misuse of confidential information are among the four or five most common types of allegations made to the CCC

Allegation data

A review by the CCC of complaints from 2009–14 identified unauthorised disclosure of information as one of the major corruption issues facing the Queensland public sector.



Recent data analysis confirms that complaints about misuse of confidential information continue to be among the four or five most common types of allegations made to the CCC. In this financial year alone, 483 such allegations have been received and, as can be seen from the graph above, this type of allegation is not only increasing in number but is also an increasing percentage of all allegations of corrupt conduct received by the CCC (7% in 2014–15 to 11.5% in 2016).



Given the prevalence of these allegations, the CCC recently audited how a group of agencies had handled the less serious complaints about confidential information that the CCC had referred to them for investigation. The audit examined the investigations of 50 complaints by eight agencies representing the sectors with the highest volumes of such incidents — departments, public health services and statutory authorities.

No agencies took the opportunity to analyse their existing preventative measures in light of the breaches

Agencies generally were not regarding breaches of confidential information seriously enough

Audit findings

The CCC found that agencies need to improve the way they deal with corrupt conduct complaints involving inappropriate access/disclosure of confidential information, to address appropriately the desired outcomes and reduce corruption risks. The CCC found that agencies generally were not regarding breaches of confidential information seriously enough or properly understanding the risks such breaches involved for the individuals concerned or their agencies. For example:

1. Confidential information that had been improperly accessed included tendering and recruitment information, personal health records, custody information, criminal histories and prisoner transfer dates. In most cases, the information had also been disclosed to others who had used it in business dealings, gaining employment, and getting favourable outcomes in court proceedings such as WorkCover claims or child custody.
2. Agencies' policies, procedures and other relevant material used to guide case officers in undertaking investigative or other resolution processes were either inadequate or required updating, to ensure that complaints were dealt with appropriately. Inadequate policies and procedures made it more likely for case officers to miss relevant evidence, make inappropriate decisions, or miss opportunities for preventative action.
3. Most employees being investigated for breaching confidential information had no restrictions placed on their access to confidential information while being investigated — indicating that agencies failed to appreciate the seriousness of such behaviour. In cases where it is impractical to block or restrict access – meaning that an officer would be unable to perform their job function — those circumstances should be documented in the decision-making process to enhance transparency and support the decision.
4. Final outcomes of investigative or other resolution processes did not always reflect the official policies and any standards of practice of the agency, even where improper access had been substantiated.
5. Agencies needed to consider and take the opportunity to analyse their existing preventative measures in light of the breaches, to see how to reduce corruption risks in the future.

Case study

Systemic breach of policy

One public sector agency had reasonable policies and procedures for handling allegations of corruption but did not always apply these in making decisions about confidential information incidents.

The CCC identified six cases in which, due to the seriousness of the allegations and despite inappropriate access being substantiated in five of them, the agency should have considered taking disciplinary action. Instead, these matters were dealt with by managerial guidance (an online tutorial or similar), **irrespective of the number of times an employee had accessed information for their own purpose**. This explicitly contravened the agency's own professional conduct standards.

Repeated decision making of this kind tells staff that their managers regard abuse of confidential information as a minor matter.

Conclusion

If public sector agencies want the confidence of the public, they must ensure that their staff understand that confidential information is entrusted to an agency for identified lawful purposes, not for the personal use of its employees. The CCC's expectation of CEOs, Directors-General and supervisors is that, in the public interest, they must provide clear direction on this issue, ensure that these standards are consistently upheld, and show "zero tolerance" for behaviour that does not meet the standard. The CCC notes that the Commissioner of Police has already taken a positive step in this direction.

Crime and Corruption Commission
QUEENSLAND

Information on this and other CCC publications can be obtained from:

Crime and Corruption Commission

Level 2,
North Tower Green Square
515 St Pauls Terrace,
Fortitude Valley QLD 4006

GPO Box 3123, Brisbane QLD 4001

Phone: 07 3360 6060
(Toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ ccc.qld.gov.au

www.ccc.qld.gov.au