Corruption in the public sector – prosecution and disciplinary action in the public interest

What you should know

• All public sector agencies should have systems in place to prevent, detect and investigate corruption, and to take appropriate disciplinary action when required.

• Where there is evidence that public sector employees (including police officers) have committed criminal offences, they should be subject to the same rules as the general public – that is, they should be referred to an appropriate authority for consideration of prosecution.

• Where there is evidence of criminal offences, public sector employees may also face disciplinary action for the same conduct. However, this may be in addition to, and not instead of, prosecution for serious improper conduct.

• Poor decision-making in relation to both disciplinary proceedings and the decision to prosecute — particularly failure to act in appropriate cases — can undermine the public’s confidence in the public sector.

This publication draws on CCC case studies to illustrate when and why consideration should be given to prosecution and/or disciplinary action in cases of serious improper conduct.
Disciplinary proceedings serve a different purpose to criminal proceedings.

The role of agencies in preventing and dealing with corruption

Generally, action to prevent and deal with corruption in public sector agencies should occur within those agencies. This means that they should:

• have effective corruption prevention frameworks in place,
• act quickly to report suspected corruption to the CCC,
• work with the CCC to determine whether investigation is required, and by whom, and
• depending on the seriousness of the conduct and the outcome of the investigation, take the action deemed most suitable.

Agencies can and do investigate matters but they should be wary of falling into two areas of potentially flawed decision making:

• prematurely deciding that there is no action to be taken, that is, no investigation is warranted OR
• deciding that disciplinary action will serve the same purpose as prosecution for criminal offences.

Criminal prosecution and disciplinary action

Broadly speaking, the courses of action that can be taken at the end of an investigation are prosecution, disciplinary action, or both.¹

Disciplinary proceedings serve a different purpose to criminal proceedings. The purposes of disciplinary proceedings are to protect the public, uphold ethical standards within public sector agencies, and to promote and maintain public confidence in the public sector.

The CCC’s view is that improper conduct by public sector employees can, and should, in appropriate circumstances, also lead to the commencement of prosecution action.

The public interest will very rarely be served by forgoing criminal proceedings simply because a public sector employee is subject to disciplinary proceedings.

¹ Another outcome of an investigation may be that allegations are not substantiated and so no further action is taken, however that situation is not the focus of this paper.
Considerations in commencing prosecutions

The Office of the Director of Public Prosecutions (ODPP) publishes Director’s Guidelines, which outline the basis for the decision to prosecute. These guidelines are similar to guidelines that exist in other agencies, including the Queensland Police Service. A prosecution should not proceed if there is no reasonable prospect of it being successful. This consideration is based on the strength of admissible evidence.

A second consideration relates to the public interest. If there is sufficient reliable evidence of an offence, discretionary factors may nevertheless dictate that a prosecution should not be commenced in the public interest. There are a number of potential discretionary factors, including the availability and efficacy of any alternatives to prosecution. The CCC is aware that this factor has, on a number of occasions, been used to justify not commencing a prosecution where disciplinary proceedings had been commenced.

However, the CCC considers that the availability of disciplinary proceedings, by itself, should rarely, if ever, justify declining to commence prosecution proceedings in the public interest. The Director’s Guidelines state that:

*The more serious the offence, the more likely that the public interest will require a prosecution.*

*Indeed, the proper decision in most cases will be to proceed with the prosecution if there is sufficient evidence. Mitigating factors can then be put to the Court at sentence.*

In relation to public sector employees, it is relevant to note that many, including, for example, police officers and others involved in the administration of justice, will be in a better position than most members of the community to ascertain what the law is and ensure they follow it. This, of course, is a factor that strongly suggests that a prosecution of public sector employees who hold these types of positions would be in the public interest, where improper conduct that constitutes an offence has occurred.

When considering investigation outcomes that provide evidence of criminal offences, public sector agencies should ensure that:

- They understand the different purposes served by disciplinary action and criminal prosecution, and that the use of one does not preclude the other.
- They do not prematurely decide that no investigation should be conducted.
- They do not pre-empt the decision about whether prosecution would serve the public interest or would ultimately be successful.
- They refer matters to the appropriate authority to determine whether there is a case for prosecution.
Prosecution case studies

The following case studies are recent examples of investigations which involved a decision about whether to prosecute and/or take disciplinary action.

Case study

Inappropriately accessing confidential information

In June 2017, the CCC was notified that a legal officer had allegedly inappropriately accessed confidential information in connection with a fraud investigation with which they had no professional involvement.

The CCC referred the matter to the legal officer’s Department and recommended it consider reporting the matter to the police service. Further investigation by the Department raised other allegations that the legal officer had failed to declare their friendship with the alleged perpetrator of the fraud. The legal officer allegedly failed to disclose the relationship when directing other staff members to provide them with updates on the case, and then used the department’s resources for personal use in accessing the alleged fraudster’s records.

After some time had passed, in September 2017, the CCC itself referred the matter to the police service.

In December 2017, the CCC were advised that the Department’s investigation substantiated the allegations and the matter was to progress to a discipline hearing. The legal officer was later sanctioned for their conduct.

The CCC was concerned that the sanction did not adequately reflect the seriousness of the conduct. On the basis that the legal officer was in a position of trust when accessing confidential information, the CCC enquired as to any decision to prosecute the officer for computer misuse. The CCC was advised by the Department that the police service had decided there was insufficient evidence to prosecute.

Although no further action was taken against the legal officer, the Department understood the CCC’s position that incidents of accessing confidential information held on computers should be referred to the police service for consideration of criminal prosecution.

Incidents of accessing confidential information held on computers are now regularly referred to the police service for criminal prosecution.
Where police refuse to enforce legislation aimed at protecting the public, the CCC believes it will always be in the public interest to prosecute.

Case study

Refusal to enforce legislation designed to protect the public

In July 2016, uniformed police witnessed a driver of a car commit a moving traffic offence. On stopping the vehicle the officers identified that the driver had been drinking alcohol and requested a breath test. The driver of the vehicle falsely identified himself as a serving interstate police officer and asked for preferential treatment. The uniformed officers initially refused the request until two plain-clothes detectives attended the scene. As a result of influence exerted by the detectives on the uniformed officers, police did not carry out a breath test, moved the driver’s car and allowed him to walk back to his holiday apartment. No prosecution action was taken against the driver.

The uniformed officers initially refused the request until two plain-clothes detectives attended the scene. As a result of influence exerted by the detectives on the uniformed officers, police did not carry out a breath test, moved the driver’s car and allowed him to walk back to his holiday apartment. No prosecution action was taken against the driver.

The incident, including the conduct of the detectives, was captured on police body worn cameras. The matter was later reported to the CCC.

Following action by the CCC, the two detectives were charged with refusing to perform a duty. The detectives received substantial fines and are currently subject to discipline action.

Case study

Computer hacking and misuse to access confidential information

In February 2016, the police service discovered that a serving member was in a de facto relationship with a member of an outlaw motorcycle gang (OMCG) who had several convictions. The officer failed to disclose this relationship, including the fact they were living together.

The initial police investigation identified that the police officer had accessed the police QPRIME database, viewed her partner’s record and falsely made an entry in the database that she had “street checked” and “breath tested” her partner. It transpired that these entries were made to hide the unauthorised searches of her partner’s records. Due to the serious nature of the allegations the CCC monitored the police investigation.

The officer was subsequently charged with computer hacking and misuse and then resigned. The officer later pleaded guilty to the offences and was fined. The police service made a post-separation disciplinary declaration that, had the officer remained a member of the police, then she would have been dismissed.