CORRUPTION PREVENTION ADVISORY

Use of official resources

Introduction

Official resources are those paid for and owned by a public entity. They may be assets, services or consumables, and can be either tangible (e.g. stationery, equipment or public housing) or intangible (e.g. information, internet access or employee time). These resources are intended to help employees carry out tasks associated with their work and provide efficient service to the community. They are not provided for the personal benefit of employees.

Using official resources appropriately is fundamental to public sector employees' legal and ethical obligations to act in the public interest, as mandated in the *Public Sector Ethics Act 1994*. Under the principles of promoting the public good, and accountability and transparency, employees are required to use and manage public resources effectively, efficiently and economically.

Appropriate use of official resources is also a requirement in the *Code of Conduct for the Queensland Public Service* and codes of conduct for local governments and other public entities.

Poor management, deliberate misuse or diversion of official resources for non-approved purposes is a breach of public trust and may result in disciplinary action or prosecution.

The resources most at risk include:

- credit cards, cash, and other public funds
- vehicles, plant, equipment and premises
- information and communication technology (ICT)
- information and intellectual property
- surplus and obsolete assets (including assets awaiting disposal)
- consumables, and fixed or movable assets
- allowances and other entitlements
- work time.

The corruption risks associated with misuse of official resources will depend on the types of resources your public entity owns or controls, the level of access employees have to them, the discretionary authority that your staff have when using them, and the harms that could result from any misuse.

Corruption risks

Improper use

Many public entities permit limited, specified personal use of the agency's resources (including mobile phones or vehicles) by employees. However, the use of any asset by a person who is not the employee, such as their family members or friends, is not authorised.[1]

Other examples of improper use include:

- Accessing personal and confidential information held by the public entity for unapproved or non-work-related reasons
- Diverting resources approved for use in one area or project to a different unapproved use
- Using work time for non-work-related activities
- Using official resources for improper personal use, such as vehicles or equipment for non-work-related activities or unauthorised use out of work hours
- Using personal issue portable assets for an unauthorised purpose, such as IT equipment such as iPads or other tablets and notebooks, cameras and smart phones or other tools and equipment.

Stealing

Work undertaken by the CCC has identified many instances where employees have taken things from the public entity for their own use, to give to someone else, or to sell. Common excuses include: "it's not used anymore and was going to be dumped", "no-one was using it", or "there's plenty in stock and I didn't think anyone would miss one or two of them".

Regardless of the resource's quantity, location or condition, employees taking something that does not belong to them is stealing, and includes:

- Stealing money from takings or petty cash, or by short-changing customers
- Borrowing funds or goods, even if there is a genuine intention to make restitution
- Using public entity resources (including tangible resources such as stationery and equipment, and intangible resources such as time or commercial in-confidence information) for other employment
- Stealing goods or equipment such as low-value small items or taking resources that have been retired from active use, including equipment that is superseded, technologically obsolete, worn or damaged, or is otherwise not used and awaiting disposal.

Fraud

Examples of fraud involving the misuse of official resources include:

- Falsifying or manipulating documents to dishonestly obtain payments (such as by colluding to submit false or inflated invoices)
- Using a public entity credit card for personal advantage
- Deliberately over-ordering resources with the intention of misusing the surplus goods or to gain other benefits such as loyalty points or tangible rewards

[1] The exception to this would be an emergency or life-threatening situation.

- Deliberately accelerating the depreciation of an asset, causing it to be disposed of before the end of its useful life, and colluding with the asset purchaser to split the proceeds when it is subsequently sold at market value
- Manipulating weak or inadequate security procedures or altering policies, procedures or business rules to improperly benefit the employee or a close associate
- Deliberately failing to return property when ceasing employment.

Misuse of ICT access and devices

Codes of conduct provide guidance about the behaviours expected of employees by the employer in relation to the use of work issued ICT access or devices.

Public sector employees must not:

- Use email, internet facilities or applications (apps) to:
  - harass or vilify, or carry out any form of cyberbullying
  - access pornography, gambling, or other illicit activities
  - participate in activities such as dating or gaming.
- Use email or internet facilities carelessly resulting in:
  - an increase of your public entity's exposure to phishing, malware, Trojans, ransomware, scams or hoaxes
  - inadvertent release of official or personal information.
- Use email or internet facilities dishonestly, including by:
  - lying, including deliberately omitting important details, or misrepresenting the facts of a matter
  - downloading or accessing material covered by intellectual property rights (such as music, movies, games, novels or articles) without the proper payment, permission or attribution
  - obtaining property or services online by deception.

Corruption offences

Criminal offences – If the misuse of official resources includes corrupt conduct or a criminal offence (such as stealing or fraud), employees could be charged under the *Queensland Criminal Code 1899* for offences including official corruption, misuse of a restricted computer, misconduct in relation to public office, abuse of authority and other offences. A conviction for these offences carries various penalties of imprisonment.

Disciplinary offences – Misuse of official resources is a breach of the Code of Conduct or your public entity's policies, and may result in disciplinary action, up to and including dismissal.

Strategies to prevent corruption

It is far better to prevent corrupt conduct from occurring in the first place than to deal with it when it does.

Strategies to prevent corruption depend on management's willingness to implement and monitor those strategies and to enforce your public entity's penalties for non-compliance.

Each public entity should conduct a detailed risk assessment to identify areas of vulnerability, and develop a range of policies, procedures and controls to assist in managing these risks.

In developing policies, procedures and codes of conduct, you may wish to model some provisions on the baseline set out in the *Code of Conduct for the Queensland Public Service*.

The following strategies to prevent corruption are not exhaustive.

Reinforce the importance of ethical conduct

Managers must set and enforce the standards of behaviour of the staff for whom they are responsible, in accordance with their public entity's rules, and can do so by:

- Setting clear rules that translate the integrity and performance obligations set out in over-arching legislation, standards, codes or directives[2] into well thought-out policies and procedures.
- Delivering structured training in integrity and use of official resources policies during induction and at regular intervals thereafter.

  Note: For staff in specialist or sensitive roles, tailored and more frequent training may be required. This training should be supported by records evidencing staff participation and their acknowledgement that they participated in and understood the training. These records will assist later in the event an investigation is launched into alleged wrongdoing.

Prevent improper use of resources

Ensure that staff are aware of their obligations in relation to use of official resources and the consequences of unauthorised or improper use. Policies and procedures should make it clear that:

- Expenditure approvals must be multilayered, and that staff cannot rubber stamp each other's spending.
- Timesheets, job sheets, vehicle logs and other official timekeeping systems must be conscientiously kept, checked and verified to prevent timesheet fraud or fraudulent claims for overtime. Some public entities find that using GPS tracking in vehicles is useful for verifying written records.
- Agency phones and computers, and all traffic on them, belong to the public entity, who has a legal right to monitor the use of any asset it owns and is obligated to act if these items are found to have been used improperly, illegally, or in breach of relevant policies (such as the Code of Conduct). Refer to the Queensland Government *Use of ICT services, facilities and devices policy (IS38)* and the Public Sector Commission's *Private Email Use Policy* and *Use of Internet and Email Policy* for helpful advice.
- Employees must not access or release official or personal information without authorisation.

---

[2] *The Public Sector Act 2022*, *Public Sector Ethics Act 1994*, *Local Government Act 2009*, *Financial Accountability Act 2009*, *Financial and Performance Management Standard 2019*, *Public Sector Commission Directives,* etc.

- Vehicles and equipment (such as phones, laptops, tools, etc.) issued to employees that are retained for use outside of normal working hours must have a detailed written agreement as to the extent of personal or non-work-related use that is acceptable. The agreement must include agreed thresholds above which the employee is required to reimburse the public entity for exceeding the reasonable use limit. Simply implementing the agreement is insufficient. The agreement needs to be supported by clear mechanisms for checking and verifying that the agreement is adhered to, processes that allow employees to make reimbursement payments, and disciplinary actions for non-compliance.
- Have a strong policy to limit expenditure on workplace facilities or furnishings, and on travel, catering and entertainment. Ensure that there is always a business reason for expenditure which is aligned to the operational or strategic deliverables for the public entity.

Prevent theft

- Clearly specify (in policies and codes of conduct) that stealing will not be tolerated and that the policy extends to theft of work time, stationery, computer accessories, cleaning consumables, tools and food supplies.
- Financial and asset management procedures should clearly state that borrowing funds or goods, even if there is a genuine intention to make restitution, is theft and will be treated as such.
- Put in place a clear policy regarding other employment, and clearly warn staff with external commitments against using public entity resources for the benefit of the other employment. These resources include tangible resources such as stationery and equipment, and intangible resources such as time or commercial-in-confidence information.
- Provide a clear policy governing the disposal of surplus, unwanted, or decommissioned goods and materials, or any items awaiting disposal, to ensure fair value is obtained and that they are not improperly written off and then sold or used for private gain. (Special attention should be given to decommissioned ICT equipment to ensure all data is properly archived as required by the *Public Records Act 2023* and is then completely and irreversibly removed from any storage or memory within the unit.)
- Accountable officers should be aware that the *Financial and Performance Management Standard 2019* requires that written records must be kept of any loss, including details of any action taken to remedy the entity's internal controls, and any material loss[3] resulting from a criminal offence or as a result of corrupt conduct must be reported to the Queensland Police Service, the CCC, the Auditor-General, and the appropriate Minister.
- Clearly document cash handling procedures (in an approved cash-handling procedure) and strictly observe these to minimise the risk of stealing from the public entity or its customers. Adequate training and supervision are vital as is the need for unannounced spot checks to ensure compliance with the procedure.
- Clearly document processes for handling electronic or online payments to your public entity. Ensure that oversight and checking mechanisms are in place to prevent loss or theft of client financial records and personal information.

[3] For further details about definitions and reporting thresholds see the Local Government Regulation 2012, and the City of Brisbane Regulation 2012.

- Limit and strictly monitor out-of-hours access to workplaces and storage areas to only those with a genuine need for it.
- Maintain and regularly audit an asset register and keep inventories of resources and their location to ensure any losses are swiftly identified. Regularly reviewing these records during a risk management process helps identify any common risks that may need particular attention.

Prevent corporate card fraud

The term "corporate card" includes a credit card, fuel card and other types of official cards.

The use of corporate credit cards poses a very high fraud risk, and must be governed by strict procedures and guidelines to ensure the cards are used only for official business and never for cash advances, personal expenditure or creating a temporary loan. Putting personal expenses on the corporate card and reimbursing it later is theft. Procedures should take account of:

- the *Treasurer's Guidelines for the use of the Queensland Government Corporate Purchasing Card*
- the *Queensland Procurement Policy 2023*
- the penalties for misuse, including the requirements of the *Financial and Performance Management Standard 2019* in relation to the reporting of losses from the misuse of the corporate credit card
- the *Criminal Code Act 1899* Qld).

Policies should clearly state that dishonest use of the corporate credit card may incur penalties including imprisonment and/or fines.

Procedures should be in place when an employee leaves the public entity to ensure that all property, identity cards, corporate cards, access cards and codes on issue to them are returned to the public entity and properly accounted for.

Conclusion – Detecting and preventing the misuse of resources

Complaints and monitoring activities remain the most effective way of detecting misuse of official resources. Public entities should cultivate a culture where staff feel free, appreciated, and safe in lodging complaints about misuse of resources (i.e. corrupt conduct), as well as implementing monitoring activities as described above as strategies for preventing corruption relating to misusing official resources.

Ensuring official resources are used appropriately is fundamental to public sector employees' obligations to act in the public interest. Poor management, deliberate misuse or diversion of official resources for non-approved purposes is a breach of public trust and needs to be prevented from occurring.

Further information and resources

- *Code of Conduct for the Queensland Public Service*
- *Crime and Corruption Act 2001*
- *Electronic Transactions Act 2001*
- *Local Government Act 2009*
- *Public Records Act 2023*
- *Public Sector Ethics Act 1994*
- Public Sector Commission
  - *Private Email Use Policy*, Mar 2018
  - *Use of Internet and Email Policy*, Dec 2015
- Queensland Government Customer and Digital Group (formerly Queensland Government Chief Information Office):
  - *Use of ICT service, facilities and devices (IS38;2018),* Dec 2015
  - *Authorised and unauthorised use of ICT services, facilities and devices guideline*, Dec 2015
  - *Use of ICT services, facilities and devices (IS38) implementation guideline*, Nov 2020
- Queensland Government, *Queensland Procurement Policy, 2023*
- Queensland Treasury, *Financial and Performance Management Standard* 2019
- Queensland Treasury, *Treasurer's Guidelines for the use of the Queensland Government Corporate Purchasing Card* (June 2024)

All Queensland legislation is available at: www.legislation.qld.gov.au

Crime and Corruption Commission
QUEENSLAND

Contact details

Crime and Corruption Commission
GPO Box 3123, Brisbane QLD 4001

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

07 3360 6060 or
Toll-free 1800 061 611
(in Queensland outside Brisbane)

07 3360 6333

More information

www.ccc.qld.gov.au

mailbox@ccc.qld.gov.au

@CCC_QLD

CrimeandCorruptionCommission

CCC email updates
www.ccc.qld.gov.au/subscribe

Note: This publication is accessible through the CCC website: www.ccc.qld.gov.au