Crime and Corruption Commission
QUEENSLAND

Corruption Prevention Advisory July 2017

Use of official resources

In this advisory:

This advice highlights the risks and offences of misuse of official resources within a public authority. It covers:

- Risk factors
- Corruption offences
- Strategies to prevent corruption
- Further information and resources.

Introduction

Official resources are those paid for and owned by a public sector organisation. 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[1] 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* (s. 4.3) and other public sector codes of conduct.

Poor management or misuse of official resources is a breach of public trust, and may result in disciplinary action or prosecution.

1 *Public Sector Ethics Act 1994* s. 7(c) Promoting the public good – public service agencies, public sector entities and public officials accept and value their duty to manage public resources effectively, efficiently and economically.

Risk factors

The resources most at risk include:

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

Each organisation faces its own particular corruption risks regarding the use of resources, depending on the nature of the assets controlled or owned by the organisation, the type of work involved, and the level of unfettered access that staff have to those assets. However, there are various ways in which resources are likely to be misused.

Improper, extravagant or wasteful use

- Careless, indulgent or injudicious decisions about the use of funds or materials
- Using work time for non-work-related activities
- Excessive or uncontrolled personal use of the agency's internet/email, which can endanger your network through:
    - congestion of the network
    - entry of malicious code via the internet resulting in damage to or theft from within the network
    - corruption of the network through infected emails, USB sticks, flash drives or CDs which bypass the gateway virus checking
    - installation of unauthorised hardware or software (including apps, games and keystroke software), which can facilitate fraud and disrupt the organisation's IT platforms.
- Excessive personal use of agency resources. Examples include (but are not limited to):
    - telephones, photocopiers, and other resources for which the agency incurs direct costs
    - vehicles (e.g. excessive diversions whilst travelling to or from work, use of vehicles during work time for non-work-related activities, and unauthorised use out of work hours).
- Unauthorised use of personal issue portable assets, for example:
    - IT equipment (such as iPads or other tablets and notebooks)
    - cameras (including smart phone cameras)
    - tools and equipment.

Limited personal use of agency resources (including "personal issue" resources such as mobile phones or vehicles) is conferred on employees. The use of any asset by a person who is not the employee (including the family or friends of the employee) is not authorised. The exception to this would be where use of the asset was related to an emergency or life-threatening situation.

Theft

- 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 organisation resources for secondary employment (including tangible resources such as stationery and equipment, and intangible resources such as time or commercial-in-confidence information)
- Stealing (taking resources, including low-value small items, for personal use or for the use of another, or to sell for personal benefit) of goods or equipment.

Fraud

- Falsifying or manipulating documents to dishonestly obtain payments (such as by colluding to submit false or inflated invoices)
- Using a government 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
- Failing to return property when ceasing employment
- Manipulating weak or inadequate security procedures for personal benefit.

Cyber-ethics

Codes of conduct provide guidance about the behaviours expected of employees by the employer. *The Public Service Act 2008* and the *Public Sector Ethics Act 1994* provide guidance about appropriate conduct in both official and private capacities. Cyber-ethics is the application of this guidance to on-line conduct, and includes avoiding inappropriate or improper conduct, such as:

- Using 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 network activities such as dating or gaming.
- Using email or internet facilities carelessly resulting in:
  - an increase of your organisation's exposure to phishing, malware, Trojans, ransomware, scams or hoaxes
  - inadvertent release of official or personal information.
- Using email or internet facilities dishonestly through such things as:
  - lying 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.

Corruption offences

Code of conduct – misuse of official resources is a breach of the Code of conduct or your agency's policies, and may result in disciplinary action, up to and including dismissal.

Criminal offence – If the misuse includes corrupt conduct or a criminal offence (such as theft or fraud) you could be charged under the *Queensland Criminal Code 1899* for offences including official

corruption,[2] computer hacking/misuse, misconduct in relation to public office, abuse of authority and other offences. A conviction for these offences carries various penalties of imprisonment up to 10 years.

Strategies to prevent corruption

Each agency 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 explores some of the possible management strategies in respect of each of the main categories.

Improper, extravagant or wasteful use prevention

- Stress the *Public Sector Ethics Act 1994* obligation in your Code of Conduct, and ensure that staff are aware that wasting resources may result in disciplinary action. Follow through to ensure that wasteful practices are eliminated.
- Ensure that work systems discourage waste. Set printers and photocopiers so that double-sided printing is the default setting and ensure that recycling is easy and a normal part of office operations.
- Develop and promote a policy of "limited and reasonable personal use" of resources such as phones, internet, email, and ICT equipment issued to personnel. Ensure staff understand that the phones and computers, and all traffic on them, belong to the agency. Staff should also be informed that the agency has a legal right to monitor the use of any asset it owns and is obligated to take action if these items are found to have been used improperly, carelessly, excessively, illegally, or in breach of relevant policies (such as the Code of Conduct). Refer to the Queensland Government *Information Standard 38* (IS 38) and the Public Service Commission's *Use of Internet and Email Policy* for helpful advice.
- Where equipment (cars, phones, tablets, laptops, tools, etc.) is issued to employees to be retained outside of normal working hours, 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 agency 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 it is adhered to, processes that allow employees to make reimbursement payments, and disciplinary actions for non-compliance.
- Ensure that expenditure approvals are multilayered, and that staff cannot rubber stamp each other's spending.
- 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 organisation.
- Develop a culture that discourages wasting work time (including deliberately wasting time or delaying work in order to justify overtime claims) and ensure that time sheets, job sheets, vehicle logs and other official timekeeping systems are conscientiously kept, checked and verified. Some organisations find that using GPS tracking in vehicles is useful for verifying written records.

2 *Criminal Code (Qld)* s. 87

Theft prevention

- Clearly specify (in policies and codes of conduct) that stealing will not be tolerated.
- Clearly convey to all staff that pilfering is theft, regardless of local customs. The items most at risk are stationery, computer accessories, cleaning consumables, tools, food and alcohol.
- 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 secondary employment, and clearly warn staff with second jobs against using organisation resources including tangible resources such as stationery and equipment, and intangible resources such as time or commercial-in-confidence information for the benefit of the secondary employment.
- 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 2002* 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 2009* (s. 21 (2)) 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] (s. 21 (3)) resulting from a criminal offence or as a result of corrupt conduct must be reported to the police, 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 agency or its customers. Adequate training and supervision are vital as is the need for unannounced spot checks to ensure compliance with the procedure.
- Limit out-of-hours access to workplaces and storage areas to only those with a genuine need for that out-of-hours access and strictly monitor that access.
- Maintain and regularly audit an assets register and keep inventories of resources and their location to ensure any losses are swiftly identified. Regularly reviewing these records in the course of a risk management process helps identify any common risks that may need particular attention.

Fraud prevention

- Every agency should have a comprehensive fraud control policy linked to detailed policies and procedures for managing procurement, finances, assets and consumable goods. This policy should be based in a comprehensive risk management system, and should take account of:
  - fraud by falsifying or manipulating documents for dishonest gain, for example:
    - to obtain payments through actions such as colluding to submit false or inflated invoices, or providing false documents in support of grant fund applications
    - to obtain career advancement by claiming false skill-sets or creating false qualifications
    - to obtain false authorities such as identification documents
    - to claim for time not actually worked in order to gain time off in lieu (flex time).
  - deliberately over-ordering resources with the intention of misusing the surplus goods
  - order-splitting to circumvent policy, or to evade scrutiny and probity standards

3 For further details about definitions and reporting thresholds see the *Local Government Regulation 2012* s. 307A(4), and the *City of Brisbane Regulation 2012* s. 279A(4).

- manipulating weak or inadequate security procedures
- fraud by purporting to be the owner of official property or by purporting to collect rents, fines or other charges for the use of official property.

- The use of corporate credit cards, while convenient, poses a very high fraud risk, and therefore must be governed by strict procedures and guidelines. Staff issued with such cards require intensive training to ensure the cards are used only for official business and never for cash advances, personal expenditure or creating a temporary loan (i.e. putting personal expenses on the corporate card and reimbursing it later – this is theft). Procedures should take account of:
  - placing blocks on accounts to prevent cash advances (noting that these blocks can be ineffective or counter-productive in remote areas or for manually processed transactions)
  - the *Treasurer's Guidelines for the use of the Queensland Government Corporate Purchasing Card*
  - the *Queensland Procurement Policy*
  - the penalties for misuse, including the requirements of the *Financial and Performance Management Standard 2009* s. 21 in relation to reporting losses from misuse of the card
  - acquittal by the card-holder which includes a signed declaration that the purchases were incurred for delegated expenditure categories and were within authorised limits
  - the Criminal Code (Qld), and 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 agency to ensure that all property, identity cards, access cards and codes on issue to them are returned to the agency and properly accounted for.
- Regular efforts should be made to ensure that fraud prevention measures are widely known and that staff have adequate and regular training in the procedures.
- Cultivate a culture where staff feel free, appreciated and safe in lodging complaints about corrupt conduct of any kind which they become aware of. Complaints remain the most effective way of detecting fraud and most other kinds of corrupt conduct.

Improper and corrupt conduct prevention and cyber-ethics

- The Code of Conduct should clearly explain to staff the kinds of personal and professional conduct which are unacceptable to the agency. Staff should be aware that they can be disciplined for conduct in a private capacity which reflects adversely upon the public service.
- The Code of Conduct and ICT policies should clearly identify that disciplinary action will be taken against employees who:
  - use email or internet facilities to harass, vilify, bully, or to circulate defamatory or illegal material, lie or otherwise misrepresent the facts of a matter
  - download information from the internet in breach of copyright laws
  - use email or internet facilities for gambling, accessing pornography, other illicit activities, or other network activities such as dating or gaming
  - use email or internet facilities in ways that carelessly expose the organisation's systems and electronic platforms to malware, Trojans, ransomware, scams or hoaxes
  - access or release official or personal information without authorisation, whether this was an inadvertent or a deliberate action.
- The code of conduct should specify requirements for staff to notify the agency if they are charged with or convicted of offences that may adversely impact on their capacity to do their work or be trusted in their workplace, or that may reflect badly upon the agency. Early notification can assist the agency in managing the consequences of such an event.

Further information and resources

- *Code of Conduct for the Queensland Public Service*
- *Crime and Corruption Act 2001*
- *Electronic Transactions Act 2001*
- *Information Standard 38* (IS 38)
- *Local Government Act 2009*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- Public Service Commission, *Use of Internet and Email Policy*, Dec 2015
- Queensland Government Chief Information Office 2009, *Information Standard 38: Use of ICT facilities and devices*
- Department of Housing and Public Works 2013, *Queensland Procurement Policy*
- Queensland Treasury 2009, *Financial and Performance Management Standard*
- Queensland Treasury 2005, *Treasurer's Guidelines for the use of the Queensland Government Corporate Purchasing Card*

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

Crime and Corruption Commission
QUEENSLAND

Please contact us if you would like further detailed guidance and information on any aspect of this advisory.

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

Stay up to date

Subscribe for news and announcements:
www.ccc.qld.gov.au/subscribe

Follow us on Twitter:
@CCC_QLD