Use of official resources

In this advisory:

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 is fundamental to public sector employees' legal and ethical obligation 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 of s. 4.3 of the *Code of Conduct for the Queensland Public Service* (PDF, 455 KB) 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.

Major misconduct risks

The resources most at risk include:

- IT or communication technology
- information and intellectual property
- credit cards, cash, other public funds
- surplus or obsolete assets
- vehicles, plant, equipment and premises
- consumables, fixed or movable assets
- allowances and other entitlements
- paid working time.

Each organisation faces its own particular misconduct risks regarding the misuse of resources, depending upon the type of work involved. However, the ways in which various resources are most likely to be misused include:

Extravagance or waste

- Careless or indulgent use of funds or materials
- Misuse of paid work time for non-work-related activities
- Misuse of telephones, photocopiers, vehicles and other equipment for non-work-related purposes
- Excessive or uncontrolled use of the internet/email, which can endanger your network through:
    - non-work-related network congestion

- entry of malicious code via the internet, resulting in damage to or theft from within the network
- corruption of the network through infected USB sticks, flash drives or CDs brought in by employees, which bypass the gateway virus checking
- installation by an employee of unauthorised hardware or software (including games and key-stroke software), which can facilitate fraud and disrupt an organisation's IT platforms.

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
- Misusing organisation resources for secondary employment (including tangible resources such as stationery and equipment, and intangible resources such as time or commercial in-confidence information)
- Pilfering and theft (taking resources for personal use or for the use of another, or to sell for personal benefit) of goods or equipment

Fraud

- Fraud by falsifying or manipulating documents to dishonestly obtain payments (such as by colluding to submit false or inflated invoices)
- Fraud by misusing a government credit card for personal advantage
- Deliberately over-ordering resources with the intention of misusing the surplus goods
- Failing to return property when ceasing employment
- Manipulating weak or inadequate security procedures for personal benefit

Disgraceful conduct

- Using email or internet facilities to harass or vilify
- Using email or internet facilities for gambling, accessing pornography, or other illicit activities.

Strategies to prevent misconduct

Each agency should conduct a detailed risk assessment to identify areas of risk, and develop a range of policies and procedures 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:

Extravagance or waste prevention

- Stress the *Public Sector Ethics Act* obligation in your Code of Conduct, and ensure that staff are aware that waste is a disciplinary offence. Follow through to ensure that wasteful practices are policed.
- 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 and email. Ensure staff understand that the phones and computers and all traffic on them belong to the agency, and that the agency has a legal right and an ethical obligation to monitor and manage their use. Refer to the Queensland Government *Information Standard 38* (IS38) and the Public Service Commission's *Use of Internet and Electronic Mail Policy and Principles Statement* for helpful advice.
- Where equipment (cars, phones, laptops, tools, etc.) are issued to employees to be retained outside of normal working hours, there should always be a detailed written agreement as to the extent of personal or non-work-related use that is acceptable, as well as clear mechanisms for checking and verifying.
- Ensure that expenditure approvals are multi-layered, 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, and ensure that there is always a legitimate business reason for expenditure.
- Develop a culture that discourages wasting of paid work time, 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.

Theft prevention

- Agencies should clearly specify (in policies and codes of conduct) that stealing will not be tolerated.
- Accountable officers should be aware that s. 21 (3) of the *Financial and Performance Management Standard 2009* (PDF, 460 KB) requires that loss of more than $500 in money or $5000 in property must be reported to the police and the CMC.
- Every agency should maintain and regularly audit an assets register and keep inventories of resources and their allocation 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.
- Cash-handling procedures should be clearly documented (in an approved cash-handling procedure) and strictly observed 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.
- Pilfering is theft, regardless of local customs, and this message needs to be clearly conveyed to all staff. 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, will be treated as theft.
- Out-of-hours access to workplaces and storage areas should be limited to only those with a genuine need for that out-of hours access and that access should also be strictly monitored.
- A clear policy should be in place regarding secondary employment, and staff with second jobs should be clearly warned against misusing organisation resources including tangible resources such as stationery and equipment, and intangible resources such as time or commercial-in-confidence information.
- A clear policy should govern the disposal of surplus or unwanted goods and materials 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 completely and irreversibly removed from any storage or memory within the unit).

Fraud prevention

- Every agency should have a comprehensive fraud prevention 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 to dishonestly obtain payments (such as by colluding to submit false or inflated invoices)
    - deliberately over-ordering resources with the intention of misusing the surplus goods
    - order-splitting to circumvent policy, or to evade scrutiny and probity standards
    - manipulating weak or inadequate security procedures for personal benefit
    - 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). Procedures should take account of:
    - placing blocks on accounts to prevent cash advances (noting that these blocks can be ineffective in remote areas or manual 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 s. 21 of the Financial and Performance Management Standard 2009 in relation to the reporting of losses from the misuse of the corporate credit card
    - information on the provisions of the *Criminal Code* that 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 training in the procedures.
- Cultivate a culture where staff feel free, appreciated and safe in lodging complaints about misconduct of any kind which they become aware of. Complaints remain the most effective way of detecting fraud and most other kinds of misconduct.

Disgraceful conduct prevention

- Your 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 or vilify, or to circulate defamatory or illegal material
    - download information from the internet in breach of copyright laws
    - use email or internet facilities for gambling, accessing pornography, or other illicit activities.
- 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

- *Public Sector Ethics Act 1994* (PDF, 400 KB)
- Department of Housing and Public Works 2013, *Queensland Procurement Policy*
- Public Service Commission 2007, *Use of Internet and Electronic Mail Policy and Principles Statement* (PDF, 70 KB)
- Public Service Commission 1997, *General Guidelines for Personal Expenses and the use of Credit Cards by Public Service Employees including Chief and Senior Executives* (PDF, 105 KB)
- Queensland Government Chief Information Office 2009, *Information Standard 38: Use of ICT facilities and devices*
- Queensland Treasury 2009, *Financial and Performance Management Standard*
- Queensland Treasury 2005, *Treasurer's Guidelines for the use of the Queensland Government Corporate Purchasing Card*

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

Last updated: 28 June 2013

Contact us
Phone: (07) 3360 6060 or 1800 061 611 (toll-free in Queensland outside Brisbane)
Email: mailbox@cmc.qld.gov.au