Tip sheet for managers

Use and misuse of public sector resources

ICAC
Independent Commission Against Corruption

FEBRUARY 2008

The misuse or theft of resources by public officials is consistently amongst the top three types of suspected corrupt conduct reported to the ICAC. Misuse of resources is at the core of many of the matters investigated by the ICAC. Clearly, people who are motivated to misuse resources continue to find opportunities to do so.

Changes in the way business is done in the public sector introduce new resources and new corruption risks. Public sector agencies need to be vigilant in managing the use of their resources and regularly assess the risk areas for misuse. Public sector managers are central to this task.

What are public sector resources?

Public sector resources can be tangible, such as equipment or public housing, or intangible, such as your time. Public sector resources are paid for, owned or controlled by public sector agencies. Examples of public resources include:

- computers/internet/email
- confidential information
- telecommunication devices
- vehicles and fuel cards
- corporate credit cards and Cabcharge cards/vouchers
- files, records and archives
- stationery and other office supplies
- your time at work
- tools, machinery and equipment
- landscaping supplies
- grants and other funds like petty cash
- office furniture and fittings
- publicly funded services such as public housing, public transport, public health and legal services.

Everyone working in the public sector has a responsibility to act in the public interest and the effective, efficient and fair use of public resources is part of that responsibility. The misuse of resources is a breach of public duty and, if serious and deliberate, can also constitute corrupt conduct under the *Independent Commission Against Corruption Act 1988*.

What is misuse?

Misuse of resources can involve theft – for example, an employee stealing a laptop computer from the work place – or unauthorised use, for example, an employee misusing the computer at work by accessing confidential information from the agency's data bases or banned internet sites, or to do 'outside work'.

The misuse of resources can cause significant financial loss for agencies. However, the costs associated with misuse of resources go beyond the lost value of the particular resource. As the following case study indicates, the investigation of allegations of misuse can be time-consuming and costly to the agency, and can result in lost productivity. It can also damage the agency's reputation, diminish staff morale, and detract from the agency achieving its objectives.

Case study

A public agency received two protected disclosures alleging that the manager of a business unit favoured a female colleague and used his work mobile phone to make personal calls to her outside work hours.

The matter was investigated by the agency over several weeks. During this time the two complainants went on extended leave as they believed the agency was not handling their protected disclosures appropriately. The manager was found to have made a substantial number of calls that were not business-related, the costs of which were to be repaid to the agency. He argued in his defence that the mobile phone policy did not give enough guidance about what was reasonable personal use of this resource. The agency conceded its mobile phone policy needed clarifying and instituted a review. Nevertheless, the manager was directed to repay $400 worth of the mobile phone calls he had made.

The agency instituted a procedure to enable the complainants to return to work. It was several weeks before the workplace issues were resolved. With the ICAC's advice, the agency subsequently strengthened its procedures for handling protected disclosures.

The presence of a clear and explicit, well-implemented policy could have prevented the situation occurring, or at least enabled it to be more quickly and easily resolved.

Use of public resources – policies and procedures

To avoid improper use of public resources, agencies should tell staff how the agency's resources are meant to be used through specific policies and procedures – for example, 'use of vehicles' and 'use of communication devices' policies – and also through other documents such as codes of conduct and secondary employment policies.

The ICAC recommends that the relevant policies include:

- a definition of what constitutes public resources and/or the resources relevant to the policy; and
- any circumstances in which the personal use of public resources is permitted,[1] and:
  - the limits and conditions of that use, and
  - the responsibilities associated with personal use, for example, responsibility for maintenance, loss, damage or theft of the resource;
- the sanctions for misuse and circumstances when the police would be advised.

Procedures associated with policies should include:

- the records to be kept on how and to whom resources have been allocated;
- an audit regime for checking compliance with the policy;
- information on how and where to report misuse and loss of resources.

In addition, the ICAC recommends that employment contracts/personnel records include:

- what resources have been provided to employees as part of their contracts of employment – for example, mobile phone, laptop computer, hand tools and
- the circumstances in which these resources are to be used.

Where personal use of public resources is acceptable

Most agencies allow limited personal use of some public resources. Clearly, the extent to which personal use of resources is allowed may be affected by the nature of the agency, the type of work it does, and whether the workplace is remote or city-based.

For certain resources a 'no tolerance' policy for personal use may be in order.

Relevant policies should clearly establish what constitutes reasonable personal use and what does not. A communication devices policy, for example, might allow infrequent, brief, personal phone calls and use of the internet and email systems, but would not allow frequent and extensive personal use, electronic transmission of offensive or pornographic material or access to pornography on the internet. Certain other activities centred on the internet, such as gambling, might be specifically prohibited.

Some agencies allow selected resources to be used that, unlike telephones for example, would not normally be available for use. Borrowing a laptop to write a job application at home might be such a use. An agency may also decide to allow limited personal use of a colour photocopier. The principles for this kind of personal use, where permitted, are the same and the ICAC recommends that agencies:

- limit and record the articles that can be used in this way and ensure staff know the conditions of this use;
- limit the circumstances in which these items can be used. This could include stipulating that the resource is for personal use only, and cannot be loaned out by the borrower or used to generate income;
- limit the occasions that an individual can use a resource. A staff member should not use a public resource frequently as an alternative to purchasing this item themselves or paying a commercial firm for services, such as colour photocopying;
- ensure that written records are made and retained about the use of such resources, including requests to borrow and approvals, the condition of the resource when lent and returned, and who is responsible for any running costs, loss or damage.[2]

Key risk areas for misuse – management strategies

The ICAC's experience has shown that there are some key risk areas that increase the potential for misuse of resources.

Risk – Secondary employment

Secondary employment is associated with a number of corruption risks, among them the misuse of public resources. Problems can arise when staff are, or are thought to be, misusing resources for purposes related to their secondary employment by:

- using the agency resources for their second job, for example, their time, the telephone and computer;
- using confidential information to benefit their second job, for example, client information, or information about a forthcoming contract;
- misrepresenting their secondary employment as being affiliated with, or under the auspice of, the public employer.

Case study

An Ambulance Officer ran her own business conducting first aid classes. Her secondary employment had been approved. The Ambulance Service received an allegation that this officer wore her Ambulance Service issued uniform when she conducted these classes, used the station photocopier and other equipment to prepare the material for these classes, disparaged her Service colleagues to her students, and gave the impression that her classes were endorsed by the Ambulance Service.

During the Ambulance Service's investigation, the officer was able to demonstrate that she had an account with a local printer for the preparation of her class material. She also denied criticising her colleagues or making any false claims that her classes were endorsed by, or under the auspice of, the Service. However, she agreed that she had worn her uniform on occasions when she was on call. The officer was counselled not to wear her uniform while engaged in her secondary employment, and to always make clear to students that she did not conduct her classes on behalf of the Ambulance Service.

Managing the risks

Risk management options include:

- having a sound secondary employment policy in place, as well as referring to it in the code of conduct; [3]
- placing restrictions on the work that may/may not be approved;
- ensuring your secondary employment policy makes it clear that the agency's resources cannot be used if secondary employment approval is given;
- requiring secondary employment approvals to be reviewed annually.

Risk – Corporate cards

Corporate credit cards were introduced into the NSW public sector in 1987 for official travel and the following year their use was extended to the purchase of goods and services.

The Audit Office, through a series of performance reviews, has monitored compliance with the Treasurer's Direction for Corporate Cards and Purchasing Cards.[4] The Audit Office concluded in its 2005 review that the findings suggested there had been a deterioration in the application of controls over credit card usage since its last review in 2001. This included instances where credit card expenditure had been incurred prior to approval, and where the heads of four out of the 10 agencies reviewed had not provided certification to their Minister that their credit card expenditure was in order.[5]

The deterioration in the application of credit card controls from 2001 to 2005 indicates that individuals and agencies can become complacent over time about following policies and procedures. This can lead to a culture of cutting corners. A motivated person can exploit this lack of vigilance.

Case study

An agency discovered that an employee had incurred over $20,000 worth of unauthorised transactions on his departmental credit card. The employee told the agency that he had given his former partner the PIN of the card, and that she had made cash withdrawals to purchase illegal drugs. The agency's review of its credit card policy included banning cash withdrawals (and releasing PINs), reducing the limit of credit available on cards, and conducting more frequent reconciliations of transactions.

Managing the risks

Risk management options include:

- requiring staff to read the agency's policy governing credit card use prior to being issued with the card, and to sign a declaration that they have read and agree to abide by the policy;
- issuing credit cards for operational reasons and not, for example, for generic reasons such as an officer's seniority (or status) in the organisation;

- where appropriate, issuing credit cards for short term periods for a designated purpose; card holders may be required to keep a diary of use;
- placing limits on the credit available on each card and conducting regular reconciliations of transactions.

Risk – Surplus materials including unwanted or low-value assets

Misappropriation of surplus or low-value assets or what appear to be unwanted or forgotten items is theft. A work culture can develop where the attitude is that it's okay for staff to take these items because "everyone does it – nobody wants this stuff – it has been forgotten – management doesn't seem to care". This may lead to deliberate over-ordering of items to create a surplus. The disposal of surplus, including low-value material and assets, should be subject to clear policy and appropriate controls.

Managing the risk

Risk management options include:

- having policies and procedures in place that outline the proper disposal of its assets, including surplus and unwanted goods, and informing staff of these;
- having asset maintenance systems in place to determine when goods become surplus and/or unwanted and what their monetary value is at this point. Consider if it is commercially viable to sell the goods externally, or to dispose of them by an in-house tender;
- conducting regular reviews of the procedures for ordering goods and services, and check for compliance.[6]

Risk – Scarce and/or high-value items

The corruption risks around scarce and high-value resources also need to be managed. The ICAC's 2005 report on an investigation into matters concerning the Australian Museum showed how a cumulative failure of policy, procedures, and audits provided the opportunity for a motivated employee to steal several hundred rare and valuable museum specimens over a number of years.[7]

Unlike most utilitarian goods which depreciate over time and with use, the value of scarce goods often appreciates. This may require increased, and ongoing, security and asset control.

Managing the risk

Risk management options include:

- conducting regular valuations of resources and updating records accordingly;
- conducting inventories of resources;
- limiting who has access to these resources, and having robust systems in place which may include swipe cards, access codes and CCTV;
- conducting appropriate background checks (including criminal checks) on staff who will be responsible for working with the resources and for installing and monitoring security systems;
- conducting regular and random audits for compliance.

Implementing policies and encouraging compliance

Having policies and procedures in place that outline the proper use of resources is an essential first step for agencies to address the associated corruption risks.

However, the ICAC's investigations show that agencies do not always consistently implement their policies and procedures and/or have adequate audit and monitoring systems in place to detect breaches. These systems weaknesses have been exploited by unscrupulous public officers, often in collusion with private persons or organisations.

Proactively conducting corruption risk assessments is an important aid to good governance and a tool for agencies to minimise corrupt conduct. Risk management should be performed as a comprehensive, structured and systematic process to evaluate and address the impact of risks in a cost-effective way by identifying and assessing the potential for risks to arise. The process improves accountability for decisions, actions and outcomes in the public sector. Corruption risk assessment and management should be an integral part of an agency's risk management practices.

The ICAC provides advice on corruption risk management in its 2007 tip sheet, [title to come].

Checklist

To ensure agency resources are not misused managers can:

- Ensure codes of conduct refer to the proper use of agency resources and make it clear that improper use may incur disciplinary responses. Ensure cross references to relevant policies are included.
- Develop and maintain policies relating to agency resources, including communication devices, internet and email and data storage systems.
- Have asset management systems in place.
- Maintain and monitor registers and records that assist with the proper management of resources, and audit compliance with information security protocols.

- Cover the proper use of resources in induction and in on-going training for staff. Illustrate this training with examples of the kinds of conflicts of interest staff may come across in their use and allocation of resources, and how these conflicts should be managed.
- Conduct screening checks for staff commensurate with their positions and use of resources, including access to confidential information.
- Have internal reporting policies and procedures in place and train staff to be familiar with and to use them.
- Inform private consultants and contractors of public sector ethics, and require them to sign confidentiality agreements and declare conflicts of interest.
- Ensure that they lead by example in the proper use of resources by:
  - making sure policies and procedures exist and work effectively;
  - complying with the policies and procedures;
  - enforcing adherence to policies and procedures.

Further advice and information

For advice on use and misuse of resource issues contact the ICAC's Corruption Prevention Advice Line by calling 8281 5999 (toll free: 1800 463 909) during business hours or visit our website at www.icac.nsw.gov.au to access relevant ICAC publications:

No excuse for misuse: Preventing the misuse of council resources – discussion paper 3, Independent Commission Against Corruption, Sydney, May 2002.

Managing risk: reducing corruption risks in local government – guidelines 2, *No excuse for misuse, Preventing the misuse of council resources*, Independent Commission Against Corruption, Sydney, November 2002.

Managing conflicts of interest in the public sector – Guidelines and Toolkit, Independent Commission Against Corruption and Queensland Crime and Misconduct Commission, Sydney and Brisbane, November 2004.

Other resources

Inappropriate use of council resources, NSW Department of Local Government Circular 06-64, 2006, www.dlg.nsw.gov.au/Files/Circulars/06-64.pdf

Model Code of Conduct for NSW public agencies, NSW Department of Premier and Cabinet, Sydney, 1997, www.premiers.nsw.gov.au/our_library/conduct/Model Code of Conduct.pdf

The Model Code of Conduct for Local Councils in NSW, Department of Local Government, January, 2005, www.dlg.nsw.gov.au/Files/Information/04-63 Model Code of Conduct for Local Councils.pdf

Personnel Handbook, NSW Department of Premier and Cabinet, Sydney, September, 2005, www.premiers.nsw.gov.au/TrainingAndResources/Publications/personnelhandbook.htm

Personal Use of Communication Devices, Part 2 of Policy and Guidelines for the use by Staff of Communication Devices, NSW Department of Premier and Cabinet, January 1999, www.premiers.nsw.gov.au/our library/conduct/compol.htm

Relevant legislation

All current NSW legislation is posted on www.legislation.nsw.gov.au.

Independent Commission Against Corruption Act 1988.

Protected Disclosures Act 1993.

Public Sector Employment and Management Act 2002.

Endnotes

1 The *Model Code of Conduct for NSW public agencies*, NSW Department of Premier and Cabinet, Sydney, 1997, p.6, states in part that "official facilities and equipment should only be used for private purposes when official permission is given".

2 *Managing risk: reducing corruption risks in local government*, guidelines: 2, *No excuse for Misuse- preventing the misuse of council resource*, Independent Commission Against Corruption, Sydney, November 2002, p.17.

3 The secondary employment policy should also refer specifically to identifying and managing conflicts of interest, as these are key factors in managing corruption risks associated with secondary employment. See, *Managing Conflicts of Interest in the Public Sector – Toolkit*, Independent Commission Against Corruption and Queensland Crime and Misconduct Commission, Sydney and Brisbane, November 2004.

4 *NSW Treasurer's Directions 205.01 – 205.08*, NSW Treasurer, Sydney, 2005. (The NSW Audit Office recommends that agencies not subject to Treasurer's Directions develop their own policies for credit card use. See *Auditor-General's Report to Parliament*, 2005, Volume 5, p.15).

5 *Auditor-General's Report to Parliament*, NSW Audit Office, Sydney, Volume 5, p 13.

6 *Guidelines for the Correct and Ethical Disposal of Scrap and Low-Value Assets*, A Best Practice Checklist – Scrap and Low Value Disposal Queensland Crime and Misconduct Commission, Brisbane, 2002.

7 *Report on investigation into the theft of zoological specimens from the Australian Museum between 1997 and 2002 and related matters*, Independent Commission Against Corruption, Sydney, September 2003.

Contact details

ADDRESS	Level 21, Piccadilly Centre, 133 Castlereagh Street, Sydney NSW 2000
POSTAL	GPO Box 500 Sydney NSW 2001
EMAIL	icac@icac.nsw.gov.au
TELEPHONE	(02) 8281 5999 or 1800 463 909 (toll free for callers outside metropolitan Sydney)
TTY	(02) 8281 5773 (for hearing-impaired callers only)
FACSIMILE	(02) 9264 5364
WEBSITE	www.icac.nsw.gov.au
BUSINESS HOURS	9.00 am to 5.00 pm Monday to Friday

ICAC

INDEPENDENT COMMISSION AGAINST CORRUPTION

ICAC tip sheet series

Tip sheets provide readily accessible and practical advice on managing and/or preventing particular types of corrupt conduct. More detailed advice can generally be found in an ICAC guideline publication on the relevant topic. The ICAC's investigation reports also provide useful corruption prevention advice that is often widely applicable across the NSW public sector. To access the full range of ICAC publications go to www.icac.nsw.gov.au/go/publications-and-resources and follow the links.