



ethics matters

in Defence Resource Management

A handbook
promoting ethical standards
and practices in resource
management in Defence

We want to hear from you!

Do you have an ethical issue you want us to address, or an experience in dealing with an ethical dilemma you want to share? Do you face difficulties when putting Defence's ethical resource management policies into practice?

The Defence Fraud Control Policy and Ethics Directorate welcomes your input—questions, comments and suggestions on ethical matters in Defence resource management.

Contact the Director, Fraud Control Policy and Ethics Directorate on 02 6266 4162, or raise your issues through the Ethics Matters 'Backchat' facility at <http://defweb.cbr.defence.gov.au/ethics>. All issues will be treated in a confidential manner.

Contents

- Foreword1
- Ethics—What they are2
- Why ethics matter in Defence3
 - Defence’s Four Unbreakable Rules4
- Leadership5
- Ethical resource management.....7
 - Waste7
 - Abuse8
 - Fraud.....9
 - Defence whistleblower scheme.....10
 - Conflict of interest.....10
 - Documentation.....12
 - Security12
- Solving ethical dilemmas15
- Common ethical concerns16
 - Defence Purchasing Card16
 - Cabcharge16
 - Commonwealth vehicles.....17
 - Commercial–in–confidence17
 - Compliance18
 - Frequent flyer points18
 - Gifts and benefits.....19
 - Intellectual property.....20
 - Internet/email20
 - Personal interests—business and shares21
 - Post separation employment.....22
 - Secondary employment.....23
 - Sponsorship.....23
- Inspector General Division25
- Legislative framework and references.....26

Foreword

An ethical culture

Public sector employment carries with it particular obligations to be responsive to Government; to be accountable; to be apolitical and professional; to deliver services fairly, effectively, impartially and courteously to the Australian public; and to manage resources efficiently, effectively and ethically. This booklet highlights the values and principles that support ethical behaviour and summarises instructions that are in place to guide you in discharging your duties and responsibilities. There are many Defence publications setting the standard for ethical conduct within Defence. This booklet refers you to the appropriate policies, instructions and statements, which are also accessible on the Defweb at <http://defweb.cbr.defence.gov.au/ethics>.

The improper use of information or position, conflicts of interest and the misuse of the employer's resources are all instances of unethical behaviour, while bribery and corruption, theft and fraud, for example, are not only unethical but are clearly also illegal.

Awareness of ethical dilemmas in the work environment should also help you to better recognise the pitfalls and areas of potential fraud, waste and abuse. An ethical environment allows commitment, competency and confidence so that when you are faced with choices on how to act, what to say or what decision to take, you are more confident about your decision—or at least you know where to seek advice and assistance.

Although many of the principles of ethics are commonsense, you may occasionally be unsure of the guidelines for doing the right thing, the right way, every time. When in doubt, seek advice before taking any action that may compromise your ethical standards or those of Defence.

This booklet reflects Defence's commitment to maintaining the highest ethical standards, but ultimately it depends on you. Please familiarise yourself with its contents and continue to uphold its standards in your work. If you have any doubts about the ethics of what you are about to do, don't proceed.

C Neumann

INSPECTOR GENERAL

July 2002

Ethics—What they are

Ethics are the principles by which our actions may be judged—good or bad, right or wrong. They include the way we make decisions when it is not completely clear what is right. And they are about doing the right thing: even when alternative options are legal and procedurally correct some choices may be better than others.

Ethics are not simply about acting according to the law or in compliance with policy; they are also about acting with consideration for values, perspective, judgment and consequences.

At work this means:

- supporting ethical work practices through our own behaviour and decision-making;
- encouraging these principles in others;
- understanding the Defence position on ethical issues;
- considering the effect of individual behaviour and the consequences of actions upon others and the organisation as a whole;
- being honest, truthful and forthright with colleagues, superiors, clients and suppliers in a manner that is sensitive to their concerns, that does not mislead them and that does not disclose confidential information;
- maintaining a high level of integrity in the face of ethical dilemmas or unethical standards in others by standing up for what is right;
- resisting pressure to do the wrong thing or to compromise these standards for short-term gain; and
- taking personal responsibility.

Our values provide a framework for ethical behaviour and support sound choices. Generally, our values help us to recognise ethical dilemmas and to sense when certain values conflict. Then we make decisions based on the relative importance of values. Our integrity helps us to make consistent and justifiable decisions that fit with Defence's values and principles.

Sometimes it helps to discuss ethical problems with other people to get a broader outlook before making a decision.

Why ethics matter in Defence

Defence is one of the largest public sector organisations in Australia. The Government and the Australian public expect us to demonstrate that we are managing our business efficiently, effectively and ethically to deliver the results expected.

Defence, through the Chief of the Defence Force and the Secretary, has given a firm commitment to the Government that Defence will manage for results, tighten accountability and improve transparency; and that all Defence staff will be responsible for their decisions and actions.

As Defence employees, we are in a position of trust with regard to using Defence equipment and resources, protecting Defence assets, maintaining security controls and procedures, and effectively reporting and documenting our activities.

Defence expects all staff to approach their responsibilities, work and dealings with colleagues in accordance with Defence's formal leadership values of:

- professionalism—exhibited by competence, dedication, commitment, morality and determination;
- loyalty—to commanders, managers, colleagues, subordinates and one's duty;
- innovation—through creativity, originality and ingenuity;
- courage—both physical and moral;
- integrity—reflecting honesty, sincerity, reliability, consistency and unselfishness; and
- teamwork—forged through equality, trust, tolerance and friendship.

The values statements for each of the Services and the *Public Service Act 1999* reinforce Defence values. Taken together they provide a sound framework for ethical behaviour that challenges us all to:

- perform our duties with skill, care, diligence, honesty and integrity;
- comply with all applicable Australian laws and with lawful and reasonable directions;
- treat members of the public and colleagues with courtesy and respect;
- avoid waste and extravagance in the use of public resources;
- disclose possible conflicts of interest and take action to avoid those conflicts;

- not use our status, duties, power, authority or inside information to gain, or seek to gain, a benefit or advantage for ourselves or anyone else; and
- not reveal any information about public business or anything that we know officially, unless we have express authority to do so.

Quite simply, Defence expects the highest levels of ethical behaviour from all members. Unethical behaviour undermines our purpose and our credibility, and can cause far-ranging consequences such as:

- loss of public trust and confidence in Defence's management procedures;
- damaged relations between Defence and industry;
- embarrassment for, and loss of confidence by, the Government and Ministers;
- poor morale; and
- lower productivity, efficiency and effectiveness.

Defence's Four Unbreakable Rules

- 1. Never mislead.**
- 2. Never abuse authority/power.**
- 3. Never 'leak' information.**
- 4. Never condone poor performance.**

Leadership

Leadership is an important aspect in promoting an ethical workplace. Commanders, supervisors and managers should ensure that:

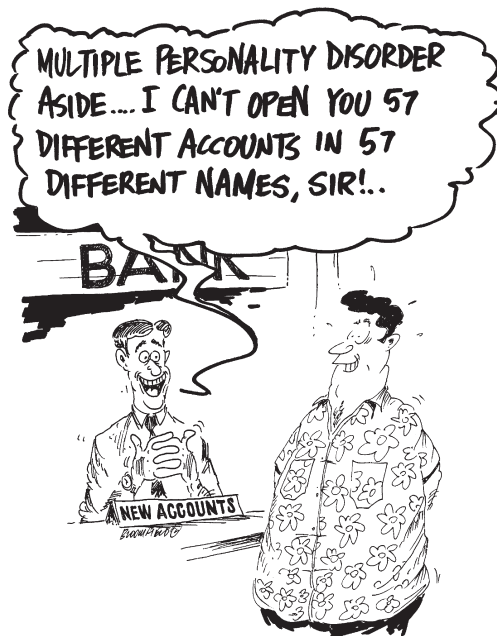
- staff understand the Defence position on ethical issues;
- they make known their own commitment to an ethical workplace and help set high ethical standards;
- they are vigilant about identifying problems and ethical dilemmas in the workplace; and
- they encourage confidence in their staff to come forward about problems or errors made on the job.

When managers promote communication and mutual respect in the workplace, staff are more likely to continue to be accountable, maintain values and integrity at work and exercise self-control. They are also less likely to compensate for a lack of recognition or appreciation by rewarding themselves in ways that may be inappropriate or even unlawful.

The following are some of the key steps commanders, supervisors and managers can take to enhance ethics and minimise inappropriate behaviour.

- Most importantly, lead by example and set the standard for ethical behaviour.
- Take responsibility where waste, abuse or non-compliance with guidelines and procedures are detected. This may require you to provide or arrange counselling, further training or disciplinary action to ensure requirements are understood and implemented by personnel. To avoid this responsibility is in itself unethical, and sends a clear message that you tolerate waste and abuse of resources or non-compliance with guidelines and procedures.
- Show personal integrity, have regard for the personal qualities of personnel, and recognise and acknowledge examples of high integrity.
- Remove or further reduce opportunities for fraud in the workplace because experience shows the majority of fraud is committed when an opportunity exists. Preventing opportunities for fraud and enhancing an ethical workplace can be achieved through:
 - education—ensure personnel receive appropriate and timely training so that rules and procedures are understood and implemented. Also, ethics training helps staff to better recognise dilemmas and appropriate courses of action;

- separation of duties—where there is potential for collusion or other fraudulent behaviour, separate key duties so that at least two staff members are required to complete high-risk duties such as purchasing, accounting and stocktaking;
- job rotation—rotate personnel to minimise reliance on one individual’s performance and reduce their exposure to possible corruption;
- documentation—ensure adequate systems and operating procedures are in place to demonstrate accountability, transparency and an audit trail;
- awareness—look for and recognise early warning signs of unethical activity. These can include a staff member refusing to take leave, resigning suddenly, using illegal drugs, habitually gambling, having persistent anomalies in work practices, or having an unusual interest in certain elements of the organisation’s business that is unrelated to their work role;



- checks—conduct routine and random checks to detect unwarranted variations to procedures, documentation, and stock and cash on hand. You may need to increase the rate of checks if new personnel are performing tasks or if procedures have changed;
- retrospective review of transactions—look for poorly prepared invoices, vague descriptions on invoices, unknown or unregistered vendors, unrecognised signatures, missing supporting documentation, cheques drawn out of sequence, access to computers at unusual times and invoices for amounts just below a threshold level;

- involvement—have greater involvement in high-risk activities and decisions. This may help you to identify work practices that need to be modified; and
- audit—conduct audits in high-risk areas. The Inspector General Division can assist in this regard.

Ethical resource management

References: *DI(G) PERS 25-6: Conflict of interest and acceptance of offers of gifts and hospitality*; *DI(G) ADMIN 10-6: Use of Defence telephone and computer resources*; the *Public Service Act 1999*; and *DI(G) ADMIN 45-2: Reporting and investigation of alleged offences within the Australian Defence Organisation*.

Proper use of Defence property, facilities and equipment is the responsibility of all Defence staff. Use and maintain assets with care and respect, guarding against waste and abuse. Avoid the use of work time and resources for purposes not directly related to Defence business. Defence facilities and equipment should normally only be used for private purposes when official permission has been given. Such use is at the discretion of the area commander, supervisor or manager. Limited personal use of telephones, facsimiles and computer terminals is allowed within current policy provisions, when it does not disrupt official work or affect operational requirements.

Waste

Chief Executive Instructions define waste as the extravagant and needless use of resources.

Resources, whether tangible or intangible, cost money to use and maintain. These include money, people, assets, time, utilities (water, electricity, gas, fuel etc.), accommodation, storage space (physical or electronic media), network bandwidth, transmission time or radio frequencies.

Examples of resource waste are:

- allowing stores such as clothing or spare parts to build-up unnecessarily;
- disposing of excess but serviceable equipment as scrap;
- storing equipment incorrectly or without regard to shelf-life, rendering the resource obsolete or unusable;

- overstocking resources, such as training aids, that are subject to continuous review and can quickly become outdated through legislation and policy changes;
- using wasteful, extravagant or unnecessary specifications in procurement;
- transmitting large files, large numbers of files or storing inappropriate data on Defence networks or terminals; and
- lavish use of consumable stores.



Abuse

Abuse is a more intentional misuse of resources and involves the exploitation of 'loopholes' to gain a benefit. Examples of abuse include:

- going interstate for training that will be available locally on another date;
- scheduling unwarranted official travel to coincide with interstate sporting or cultural events;
- using Defence vehicles for personal purposes;
- using Defence resources to support involvement in external activities such as clubs or sporting organisations; or
- using Defence communications facilities to run a business or to conduct stock exchange trading.

Fraud

Fraud is a step beyond unethical behaviour. While unethical behaviour might involve different interpretations of values or guidelines, fraud involves the misappropriation of funds, benefits or other property. It involves breaking laws or contravening instructions. The benefit obtained by fraud is often money, or something having monetary value, but may also involve the wrongful use of Defence resources or information.

The *Commonwealth Fraud Control Guidelines 2002* describe fraud against the Commonwealth as 'Dishonestly obtaining a benefit by deception or other means'. This definition includes:

- theft;
- obtaining property, a financial advantage or any other benefit by deception;
- causing a loss, or avoiding or creating a liability by deception;
- providing false or misleading information to the Commonwealth, or failing to provide information where there is an obligation to do so;
- making, using or possessing forged or falsified documents;
- bribery, corruption or abuse of office;
- unlawful use of Commonwealth computers, vehicles, telephones and other property or services;
- relevant bankruptcy offences; and
- any offences of a like nature to those listed above.

The benefits referred to can be either tangible or intangible. Examples include:

- hacking into or interfering with a Commonwealth computer system;
- using a false identity to obtain income support payments;
- using Commonwealth systems to gain access to other systems without authority;
- charging the Commonwealth for goods or services that are incomplete or not delivered;
- hiding or disposing of assets by bankrupts to avoid paying creditors; and
- making false statement under the *Commonwealth Electoral Act 1918*.

Defence has a well-developed fraud control planning process in place to address these issues.

Defence whistleblower scheme

Reference: *DI(G) PERS 45-5: Defence whistleblower scheme.*

Unethical behaviour or misconduct may damage Defence's reputation or ability to operate effectively. Defence is committed to creating an ethical organisation and to ensuring that people feel able to raise concerns about misconduct or wrongdoing in an environment free of victimisation and harassment.

Ideally, alleged misconduct or wrongdoing should be reported through line management or the chain of command. Sometimes, however, people are unable to use these channels because they lack confidence in them or believe that they might be victimised, discriminated against or disadvantaged in some way if they pursue a concern.

Defence has a whistleblower scheme that applies to civilian and military members who believe that they should report alleged misconduct or wrongdoing and do not have confidence in reporting through the chain of command or line management. The whistleblower scheme allows them to disclose information directly to the Inspector General Division and to expect that their report will be investigated.

All reports are treated in the strictest confidence. Confidentiality is important for three reasons:

- to protect people from allegations not yet proven—a person has the right to privacy and protection from gossip or reprisal;
- to protect the whistleblower; and
- to prevent possible destruction of evidence.

Reports may be made in writing, in person to the Director, Investigation and Recovery, or by using the dedicated hotline—1800 673 502.

Conflict of interest

References: *Public Service Act 1999, Part 3, Section 13: Australian Public Service code of conduct; DI(G) PERS 25-2: Employment and voluntary activities of Australian Defence Force members in off-duty hours; DI(G) PERS 25-3: Disclosure of interests of members of the Australian Defence Force; DI(G) PERS 25-4: Notification of post separation employment; and DI(G) PERS 25-6: Conflict of interest and acceptance of offers of gifts and hospitality.*

Conflict of interest relates to any situation where there is, or merely appears to be, a conflict between your personal interests and the goals, objectives and values of Defence.

Conflicts of interest can take many forms and cannot always be avoided. In such circumstances, how you handle the potential conflict of interest is very important in maintaining personal and organisational integrity and public trust. The following questions may assist you in making a judgment concerning potential conflicts of interest.

- Are you using your position or authority to make decisions that result in a benefit to yourself, your family or your friends?
- Would your acceptance of a gift or benefit, no matter how insignificant it might seem, place you in a perceived conflict of interest from the perspective of other Defence employees, contractors or the public?



- If you accepted a benefit, would you still be in a position to make unbiased business decisions that are first and foremost in the public interest?
- Have such benefits been offered before, with the giver expecting favourable treatment as a result?
- Could work colleagues become concerned about or resentful of the 'perks' you appear to enjoy in your job as a result of your acceptance of benefits?
- Would visitors from outside Defence gain an unfavourable impression from a benefit or gift in your possession (such as a promotional model on your desk)?
- Would you be able to satisfactorily explain the acceptance of a gift or benefit to a parliamentary committee?

You must use your authority and the resources and information available to you only for the intended work-related purpose. Although you may think your actions are ethical, the mere perception of a conflict of interest may cast doubt on your ability to act without bias with regard to Defence and Commonwealth interests.

Your supervisor must also work actively to help resolve any conflicts of interest that occur, or may occur, in the work area. Depending on the significance of the conflict, a supervisor's options could be to:

- record the details of the disclosure and take no further action because the potential for conflict is minimal or can be eliminated by such disclosure or effective supervision;
- disqualify an individual from any decision where he or she could have either an actual or potential conflict of interest; or
- remove or transfer an individual from the duties where the conflict arises.

Many of the common ethical dilemmas discussed in later sections cover other areas where conflicts of interest may occur.

Documentation

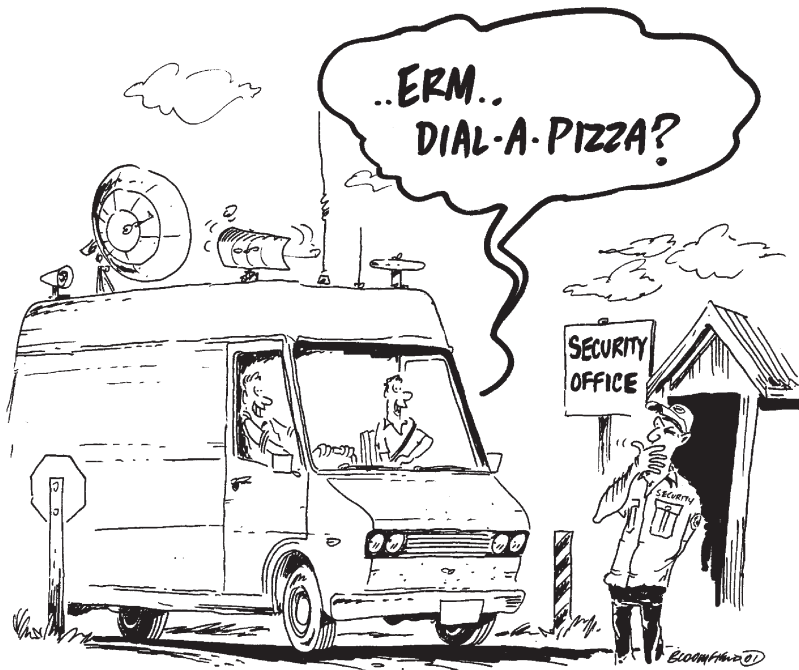
Reference: *Archives Act 1983*.

Good governance requires that everyone maintain accurate and complete records that demonstrate accountability, probity and transparency. Your actions need to be supported by well-documented decisions. Documents should be kept in a logical sequence so a clear audit trail can be followed.

Security

References: *Commonwealth Protective Security Manual 2000, Part C*; *Defence Information Systems Security Manual 3 (SECMAN3)*; *Defence Protective Security Manual 4 (SECMAN4)*; *DSI 7/99, Handling of official information*; *DI(G) ADMIN 08-1, Public comment and dissemination of information by Defence members*; *DSI 6/00, Combination lock settings*; *DSI 10/01, Access to restricted and X-in-confidence information*; and the *Criminal Code Act 1995*.

Providing good security has an important ethical dimension. The Commonwealth and Defence protective security policies outline, amongst other things, two of the security objectives that go to the heart of ethical behaviour:



- being assured, to the greatest possible extent, that only loyal, trustworthy and reliable persons of integrity and discretion, who have an established need, are permitted access to classified or sensitive Defence information; and
- preventing the unauthorised disclosure of classified and official Defence information whether deliberate or otherwise.

The unauthorised disclosure of official information, commonly known as 'leaking', may damage the trust that exists between Defence and Government, and the Australian community at large and our allies. It may adversely affect military operations and could ultimately result in avoidable casualties or compromise war-fighting capabilities.

In general, the *Crimes Act 1914* contains the legislative provisions for the protection of classified information, including official information, and the penalties for unauthorised disclosure of that information. Section 70 of the Act makes it clear that Commonwealth officers, current or former, are not to disclose any information that they are or were, at the time of ceasing to be a Commonwealth officer, bound not to disclose. The term 'Commonwealth officer' includes a person performing services for or on behalf of the Commonwealth, such as contractors.

Section 79 of the Act is concerned with 'official secrets' and makes it a criminal offence for any person to communicate official secrets (the nature of which are described in the section) to any unauthorised person. The combined effect of the Act is that the unauthorised disclosure of information held by the Commonwealth is subject to the sanction of criminal law.

The *Defence Act 1903* contains similar provisions to the Crimes Act for preserving the secrecy of information relating to any defence works relevant to the defence of the Commonwealth.

Section 13 of the *Public Service Act 1999* sets out the Australian Public Service (APS) code of conduct. That code in particular provides that APS employees must not, except in the course of their duties, give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge.

Members of the Australian Defence Force (ADF), wherever they serve, are subject to the *Defence Force Discipline Act 1982* (DFDA). As an example, ADF personnel who publicly disclose classified or official information may contravene Defence Instruction (General) ADMIN 08-1 Public comment and dissemination of information by Defence members, thereby committing an offence against section 29 of the DFDA, Failure to comply with lawful general order.

Disclosure of official information should only occur if that disclosure is authorised. Authorisation may be granted under the express authority of an appropriate appointment within a Service or Group, subject to the provisions of the *Freedom of Information Act 1982* (the FOI Act). In relation to personal information, such disclosure must be in compliance with the *Privacy Act 1988*. The FOI Act provides a legislative basis, though not an exclusive basis, to access government-held information, including the applicant's personal information.

The interrelationship between the Crimes Act, the FOI Act and the Privacy Act is significant, with a need to balance priorities in situations in which the disclosure of information could result in harm to the Government, the nation or individuals. The Privacy Act does not allow individuals to access personal information if access is not permitted under the FOI Act or the *Archives Act 1983*.

Outsourcing of many non-core activities has increased the need for Defence contractors to access Defence premises and classified information. Depending on the circumstances, contractors are allowed access to (in electronic or hard copy) classified information at the highest levels. Appropriate security procedures, based on the nature of the function and the classification of the information, need to be negotiated with the contractor and settled before finalising the contract. Contracts that involve access to security-classified information must impose on the contractor and any subcontractor an obligation to meet mandatory security requirements.

An effective security and ethical regime must be viewed as enabling the delivery of business outcomes and not as an added or unnecessary impost on resources. Maintaining Defence's knowledge edge requires an appropriate security environment, supported by a systematic and coordinated approach.

Solving ethical dilemmas

Sometimes we are faced with conflicting choices that can lead to an ethical dilemma. Such situations can be difficult and complex. They can involve two or more right courses of action, two or more optional courses of action, or two or more values that cannot both be equally well served.

So let's look at some general steps to follow whenever you are uncertain about what is the right thing to do to resolve an ethical dilemma.

1. Determine whether you actually have the authority or responsibility to address the issue.
2. Identify and explore all the options. This is a crucial step. Many people get into strife because they leap in and do the first thing that occurs to them—especially if they are under some pressure to act. You owe it to yourself to make sure you have identified all the options open to you. You will often find that, no matter how difficult a situation may appear at first, there is an acceptable way to deal with the problem.
3. Discuss the matter, and be prepared to accept advice. Most people have had to deal with ethical dilemmas at some time. Talk to someone—partner, workmate, boss—who may be able to give you advice: even if it's a lesson in how not to go about actions. (Who you talk to must, of course, be subject to normal security considerations.) The transparency that comes from sharing a problem with others is a good defence against any misunderstanding of your motives or any misperception of your behaviour.
4. Recognise the consequences of your decision. Even if you feel justified in making a certain choice, ask yourself who or what will be affected by your decision, and whether any harm will be done. Is there a way to avoid or at least to minimise harmful consequences while enabling you to achieve your objectives?
5. Own the decision once it is made. Accept that the decision has your name on it, and don't try to pass it off as the result of some sort of automatic bureaucratic process. Be aware of your responsibility, particularly when exercising delegations.
6. Be prepared to justify your decision. You may have to answer questions about your decision from a superior, an auditor or Parliament.

Common ethical concerns

There are a number of issues that commonly arise as areas for concern in the ethical management of Defence resources. These are addressed briefly in the next few pages. In each case, references have been provided to guide you towards more detailed advice on the issue.

Defence Purchasing Card (formerly Australian Government Credit Card or AGCC)

Reference: *CEI, Vol. 2, Part 6, Chap. 2: Australian Government Credit Card.*

Defence Purchasing Cards must not be used for personal purchases. To do so and try to justify it by saying you will pay the amount back immediately or within the billing cycle is prohibited. Whether or not interest accrues to the Commonwealth is not the point—to use a Defence Purchasing Card for other than Commonwealth purchases is illegal. The *Financial Management and Accountability Act 1997* provides for a maximum of seven years of imprisonment for wilful and deliberate misuse.

Cabcharge (vouchers and cards)

Reference: *CEI, Vol. 2, Part 7, Chap. 4: Accountable forms.*

Cabcharges must only be used for official travel and when it is more efficient than hiring a car. For example, while it is more cost-effective to hire a car for travel between Perth airport and Garden Island at Rockingham, it is probably cheaper to use Cabcharges in busy cities where parking is expensive and hard to find. Cabcharges should not be used for travel associated with mess functions or social club dinners or any other non-official functions.



Commonwealth vehicles

References: *CEI, Vol. 2, Part 9, Chap. 9: Charges for home garaging Commonwealth vehicles*; *DI(G) ADMIN 20-28: Defence road transport instructions*; and *DI(G) LOG 01-11: Defence executive vehicle scheme*.

Commonwealth vehicles should only be used to facilitate the performance of duties and be to the benefit of the Commonwealth rather than the individual. Under normal circumstances vehicles should not be used for private purposes such as travel from home to work. When not in use, official vehicles should normally be garaged on official premises. Approval to vary this policy may be granted under certain circumstances.

Commercial-in-confidence

Reference: *DI(G) ADMIN 08-1: Public comment and dissemination of information by Defence members*; *DSI 7/99: Handling of official information*; and *DCM 32/00: Setting the standard in communications*.

Unauthorised disclosure of information may cause harm or give an individual or an organisation an improper advantage. It can also damage Defence's reputation, integrity and credibility if it is seen that information is not secure.

Information supplied by companies and defence businesses is usually given in confidence and on the strict understanding that it will not be revealed to anyone other than those with a genuine need to know. Under no circumstances are you to allow commercial-in-confidence information to be made known to unauthorised persons. Competing companies are never to be given another company's information in regard to performance specifications or any aspects of pricing, quotation, tender, advance details of future product releases, or any other commercial or proprietary information.

Keeping information secure applies to Defence information, too. Official information must only be used for the intended work-related purpose and not for personal benefit. 'Leaking' or the unauthorised disclosure of official information is illegal.

Confidential information may be written, stored on a computer, or might be something that you overhear or are told at work, for example, information about other agencies, or information about government decisions which provide an unfair advantage in buying property or shares. Therefore, you need to be vigilant about the security of Defence information.

Compliance

References: *Public Service Act 1999, Part 3, Section 13: Australian Public Service code of conduct; Defence Act 1903, Section 9(a); Defence Force Disciplinary Act 1982, Part III, Section 29; and DI(G) ADMIN 01-1: The system of Defence instructions.*

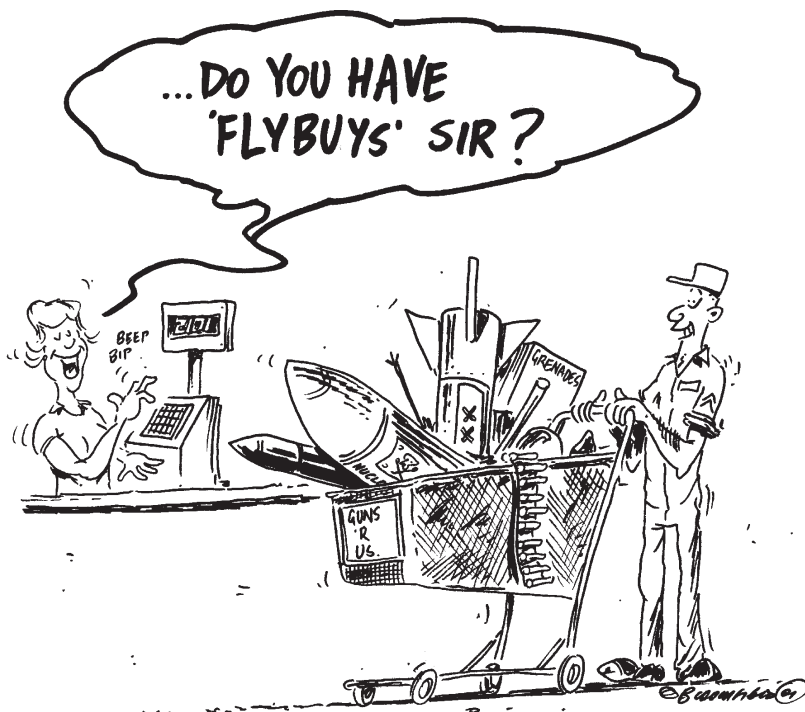
You must comply with all applicable legislation, policies and principles that relate to external and internal activities associated with the system of government, and implement the policies and decisions of the Government in an impartial manner.

Frequent flyer points

References: *DEFGRAM 51/00: Travel—Changes under new contract.*

Frequent flyer points accrued from publicly funded travel must not be used privately or for upgrades above your travelling entitlement. You should tell your travel booking area of any points that have accrued. Points cannot be redeemed on leaving Defence.

From February 2000, points no longer accrue from official travel; however, existing points should still be redeemed for such travel.



Gifts and benefits (including hospitality, travel and accommodation)

Reference: *DI(G) PERS 25-6: Conflict of interest and acceptance of offers of gifts and hospitality.*

In the private sector, gifts and benefits are often considered conducive to good working relationships. In the public sector, accepting such things can raise probity considerations such as the potential for conflict of interest or the effect a gift or benefit may have on your ability to perform your duties in an unbiased way. This is true whether or not any favours are actually extended or exchanged.

Gifts and benefits offered can range from low-value items such as calendars or pocket diaries, to more expensive things such as meals, entertainment, accommodation, travel and costly promotional items. You must always inform your supervisor when any offer of a gift is made, even if you do not accept it. This ensures you are acting with transparency and probity.

As a general principle, Defence staff should not accept offers of gifts other than those of an inexpensive nature and only when this could not be construed in any way as leading to a conflict of interest, favouritism or preferential treatment for either party.

It is not appropriate for Defence personnel to accept any offer of free entertainment if it could be regarded as substantial or could give rise to either the reality or perception of a conflict of interest. The exchange of only modest hospitality by Defence and other organisations is appropriate as a means of facilitating business. But even this requires prior approval. Cost sharing can also be appropriate, for example, pay for your own dinner. Accepted hospitality should never be lavish, nor should it include travel and accommodation.

Defence staff should never solicit gifts, benefits or hospitality for themselves or for any other person or organisation.

If an organisation with which you deal wants to provide a gift such as a model or sample, this should be given to the Defence area concerned rather than to an individual—gifts of this kind must be registered in accordance with procedures set out in the *Chief Executive Instructions*.

Defence meets the business travel and accommodation requirements of its personnel who are carrying out official business. A supplier can provide such items in exceptional circumstances only, such as travel to a remote location that can only be reached by a company aircraft.

Intellectual property

Reference: *Getting smarter about knowledge rights* [Defence Intellectual Property Policy Statement, June 1999].

Intellectual property is a broad term covering products or outcomes arising from creative or innovative human effort. This could include designs and drawings, computer software, inventions, books, reports, technical information and photographs. It can also be confidential or commercial-in-confidence information.

Intellectual property is increasingly recognised and regarded as a business tool and as a source of profit and competitive advantage. It is an area in which conflict of ownership may arise between the employee who developed a product or concept and the employer.

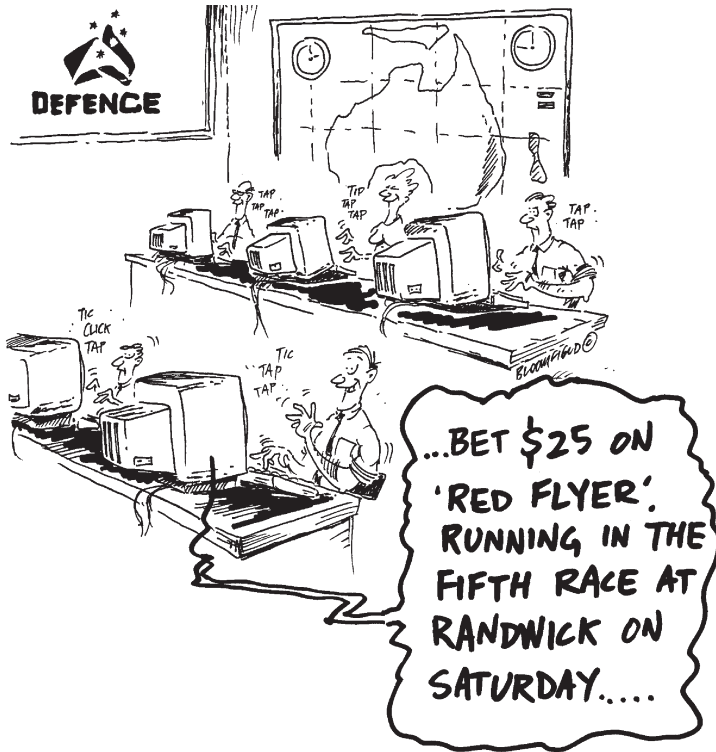
In broad terms, all material that is produced by Defence members, at work or under the direction and control of Defence, remains the intellectual property of Defence.

Internet/email

Reference: *DI(G) ADMIN 10-6: Use of Defence telephone and computer resources; DIMPI 5/01: Defence information environment, provision of Defence email and internet services; and DI(G) ADMIN 08-1: Public comment and dissemination of information by Defence members.*

Internet and email services provided within Defence are primarily for official use but some limited personal use is allowed. For example, email may be used to converse with your child's teacher, but it is not provided for aimless chat or to distribute humorous video or audio files to others. Similarly, the internet may be used to access banking sites to conduct personal transactions or pay bills, but downloading the latest games software is not appropriate.

Inappropriate use of Defence resources is not only an obvious waste of the organisation's time and money—it may also be illegal in some cases. The provision of internet and email facilities (and the bandwidth that they use) is, like all other resources, funded by the taxpayer, and there is a strong and correct expectation that these resources will be used in a responsible manner.



Personal interests—business and shares

References: *DI(G) PERS 25-2: Employment and voluntary activities of Australian Defence Force members in off-duty hours*; and *DI(G) PERS 25-3: Disclosure of interests of members of the Australian Defence Force*.

If you or a family member (even extended family) have holdings, directorships, trusts or shares in companies that do business with Defence, you must avoid any financial or other interest that could compromise your impartial performance of duties. If you are not sure whether a conflict exists, you should discuss the situation with your supervisor.

Supervisors also have a responsibility in helping to resolve conflicts of interest or perceived conflicts of interest.

Post separation employment

Reference: *DI(G) PERS 25-4: Notification of post separation employment.*

Post separation employment refers to situations in which Defence employees leave the organisation (including discharge from a Service) to take up appointments with private or public sector organisations that provide or intend to provide services, supplies or materiel to Defence.

As a Defence employee, you must not use your position to obtain opportunities for future employment. This means you should not allow yourself, or your work, to be influenced by plans for, or offers of, employment outside Defence.

Of course, if you leave Defence you are free to use the skills you acquired. It is generally in Defence's interest to have people in industry with Defence expertise and experience. However, sometimes your knowledge and contacts could give you an unfair commercial advantage. Remember, you must not use confidential information gained while you were working in Defence, unless that information is now public.

To ensure probity and transparency, you need to consider three issues in seeking or negotiating employment upon leaving Defence:

- protection of confidential information that was gained by virtue of your former Defence position;
- potential for inappropriate use of departmental contacts or personal influences to secure preferential treatment for a new employee; and
- actions or decisions you made, while still employed by Defence, that may be construed as giving preferential treatment to a company in anticipation of you receiving an offer of employment from that company in the future.

To reduce the potential for embarrassment to yourself, Defence and the prospective employer, you should follow the post separation procedures in *DI(G) PERS 25-4*.

You must also be careful about working with former employees. Make sure you do not give them, or appear to give them, favourable treatment or access to privileged information.

The Commercial Support Program Handy Hints, which form part of the *CSP Manual*, include other guidelines on post separation employment for employees working in areas that are being outsourced.

Secondary employment

References: *DI(G) PERS 25-2: Employment and voluntary activities of Australian Defence Force members in off-duty hours*; and *DI(G) PERS 25-3: Disclosure of interests of members of the Australian Defence Force*.

Outside work (whether paid, unpaid or voluntary) may be carried out only if you have permission from Defence and only where this work does not conflict or interfere with your official duties. Outside employment includes paid work such as tutoring, driving a taxi, running a business or other paid activities such as holding a directorship. Unpaid voluntary work that has the potential to create a conflict of interest is also included. All outside employment (paid or voluntary) is to be performed wholly in your private time.

You must obtain permission to hold a second job, even during periods of long service or recreation leave. When discussing this with your supervisor or superior, you should be able to prove that taking the position will not create a conflict of interest or affect the performance of your Defence work. You are responsible for advising your superiors of actual or potential conflicts of interest, for example, where information about Defence, its clients or procedures would be useful in that job or to the employer.

Sponsorship

References: *DCM 53/98: Guidelines on conflict of interest issues for Defence personnel*; *DI(G) PERS 25-6: Conflict of interest and acceptance of offers of gifts and hospitality*; and *DI(G) PERS 25-2: Employment and voluntary activities of Australian Defence Force members in off-duty hours*.

DI(G) PERS 25-6 notes that sponsorship of such things as Defence conferences, symposiums, social and sporting club activities, and activities of a charitable or public benevolent nature are part of the Defence culture. These types of sponsorship can be cause for concern when:

- approaches to private sector organisations could be perceived as an attempt to exert pressure on them to provide donations and when a refusal could be seen as prejudicing their relations with Defence;
- the acceptance of sponsorship could be seen as giving some organisations preferential access or status with Defence; or
- there could be a real or apparent conflict of interest.

Put simply, Defence does not allow you to accept or seek sponsorship or commercial endorsement relating to events, functions, products or businesses when this could give rise to a perception of real or potential conflict of interest for Defence or another party. Such action could give the appearance that Defence is recommending a business or promoting use of a product; it could also diminish our perceived capacity to act in an unbiased, independent way towards any and all potential suppliers.

Defence may, however, seek to recover the cost of providing venues for industry-sponsored trade displays or meetings that are conducted on Defence property. Defence employees must ensure this recovery action is transparent by recording it through appropriate Defence accounting processes.



Inspector General Division

The Inspector General Division conducts independent reviews, audits and evaluations of Defence activities, and works to assure accountability within Defence. Of course, these activities are not remedies for ineffective management. Reporting and monitoring tools must be supported by everyone's commitment to an ethical culture.

To enhance this support, the General Investigations and Review Branch of the Division deals specifically with ethics and fraud. It includes:

- the Investigation and Recovery Directorate which investigates allegations of fraud and misconduct, questions of probity and breaches of process, and which administers the Defence Whistleblower Scheme. Its Director can be contacted on 02 6266 4590; and
- the Fraud Control Policy and Ethics Directorate which develops policy relating to an ethical working environment, manages a Defence-wide awareness program in ethical resource management, develops fraud control policies and the Defence Fraud Control Plan, and assists Groups to develop and implement fraud control plans which can more effectively minimise fraud and abuse. Its Director can be contacted on 02 6266 4162.

Some elements of the Defence-wide ethics awareness program are:

- this handbook;
- ethics and fraud awareness presentations and workshops;
- *Ethics matters* newsletters;
- videos on ethical and fraud-related issues; and
- a website on the Defence intranet—<http://defweb.cbr.defence.gov.au/ethics>.

Presentations and workshops can be provided, the newsletter is distributed regularly, and the website provides up-to-date information about issues in ethical resource management and the latest departmental references and guidelines. It also includes a streamlined mechanism for booking ethics presentations or workshops, and for ordering copies of publications and videos.

The Fraud Control Policy and Ethics Directorate welcomes comments and suggestions on any aspect of its programs. See the inside front cover for contact details.

Legislative framework and references

Legislation and Defence instructions also guide our ethical behaviour in the workplace. These include:

- the *Archives Act 1983*;
- the *Defence Act 1903*;
- the *Defence Force Disciplinary Act 1982*;
- the *Financial Management and Accountability Act 1997*;
- the *Public Service Act 1999*
 - Part 3, Section 10: Australian Public Service values
 - Part 3, Section 13: Australian Public Service code of conduct;
- the *Criminal Code 1995*;
- Chief Executive Instructions, Volume 2, Finance—CEI
 - Part 1, Chapter 1: Fraud control in Defence
 - Part 1, Chapter 2: Roles and responsibilities of Management Audit Branch
 - Part 6, Chapter 2: Australian Government Credit Card
 - Part 6, Chapter 3: Official hospitality and working meals
 - Part 7, Chapter 4: Accountable forms
 - Part 7, Chapter 6: Giving and receiving gifts of public property
 - Part 9, Chapter 8: Charges for hiring service messes for private functions
 - Part 9, Chapter 9: Charges for home garaging Commonwealth vehicles
 - Part 10, Chapter 4: Use of frequent flyer schemes;
- Defence Instructions (General)—DI(G)
 - DI(G) ADMIN 01-1: The system of Defence instructions
 - DI(G) ADMIN 08-1: Public comment and dissemination of information by Defence members
 - DI(G) ADMIN 10-6: Use of Defence telephone and computer resources
 - DI(G) ADMIN 20-28: Defence road transport instructions
 - DI(G)ADMIN 45-2: Reporting and investigation of alleged offences within the Australian Defence Organisation
 - DI(G) PERS 06-3: Visits to Defence establishments by organisations offering advice targeting members of the Australian Defence Force

DI(G) PERS 25-2: Employment and voluntary activities of Australian Defence Force members in off-duty hours

DI(G) PERS 25-3: Disclosure of interests of members of the Australian Defence Force

DI(G) PERS 25-4: Notification of post separation employment

DI(G) PERS 25-5: Employment of immediate family members in the same chain of command and/or working environment

DI(G) PERS 25-6: Conflict of interest and acceptance of offers of gifts and hospitality

DI(G) PERS 45-5: Defence whistleblower scheme

DI(G) FIN 12-1: The control of fraud in Defence and the recovery of public moneys

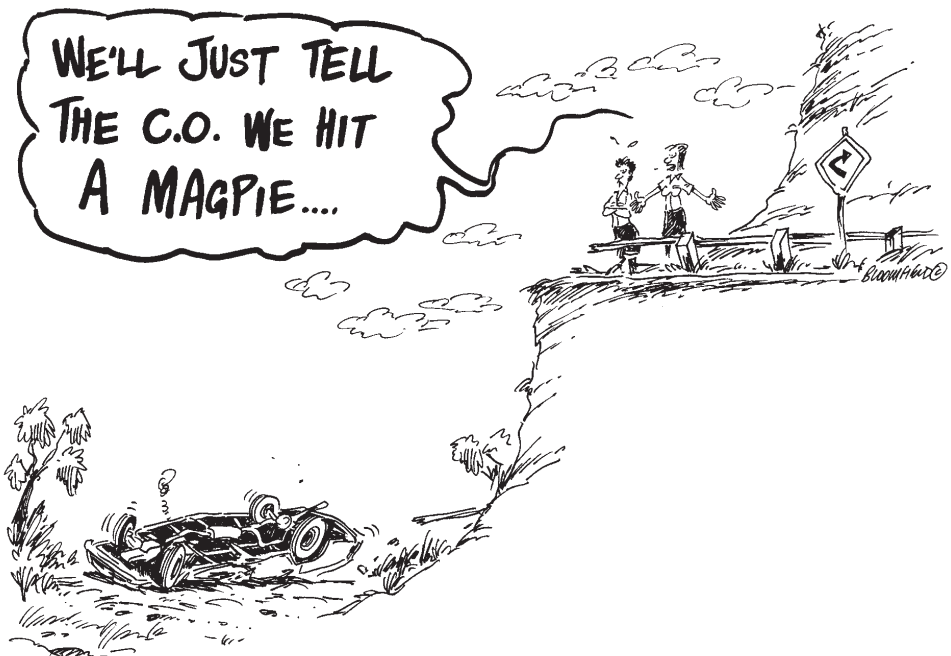
DI(G) LOG 01-9, Use of official vehicles between private residences and place of duty

DI(G) LOG 01-11, Defence executive vehicle scheme;

- Departmental Administrative Instructions—DAI
DAI 1/98: Application of Defence Instructions (General);
- Defence Information Management Policy Instructions—DIMPI
DIMPI 4/01: Telephones and related goods and services
DIMPI 5/01: Defence information environment, provision of Defence email and internet services;
- Departmental Personnel Instructions—DPI
DPI 4/91: Spouses accompanying civilian staff on short-term visits overseas and duty travel within Australia at official expense

DPI 3/99: Preventing, managing and eliminating discrimination, harassment and unacceptable behaviour in the Department of Defence;
- Departmental Security Instructions—DSI
DSI 7/99: Handling of official information
DSI 8/99: Personal responsibility for security [information]
DSI 6/00: Combination lock settings
DSI 10/01: Access to restricted and X-in-confidence information;
- Defence security manuals (SECMAN)
SECMAN3: Defence Information Systems Security Manual 3
SECMAN4: Defence Protective Security Manual 4;

- Defence Circular Memorandums—DCM
 - DCM 53/98: Guidelines on conflict of interest issues for Defence personnel
 - DCM 05/00: Defence travel arrangements
 - DCM 32/00: Setting the standard in communications;
- DEFGRAMs
 - DEFGRAM 51/00: Travel—Changes under new contract
 - DEFGRAM 43/02: 'Free' \$100 gift certificate; and
- other reference documents
 - Defence Fraud Control Plan
 - Defence and industry—An ethical relationship
 - Commonwealth Protective Security Manual 2000, Part C
 - Defence Procurement Policy Manual (Version 3)—especially Section 2, Chapter 3: Ethics and fair dealing
 - Getting smarter about knowledge rights [Defence Intellectual Property Policy Statement, June 1999]
 - Commonwealth Fraud Control Guidelines 2002.



ethicsmatters

ethicsmatters

in Defence Resource Management

Visit our website: <http://defweb.cbr.defence.gov.au/ethics/>