Supplementary exhibit: A Code of Conduct for New Zealand Police

Extracts from other New Zealand Police policies, post 2008

1. From the Professional Distance Policy (effective from 2 December 2008)

This policy provides further guidance and clarification on the relationships between members of the public and Police employees and between two Police employees.

Description

The nature of policing means conflicts of interests and power imbalances may occur. The purpose of this policy is to provide guidance on managing and limiting risks to individual employees and to Police where a conflict of interest or power imbalance may arise in relationships.

While some of these issues can be resolved by taking appropriate steps, other relationships will always be unethical.

In certain circumstances, the development of a personal relationship between Police employees and members of the public that they have come into contact with through a professional relationship may be inappropriate, particularly where a sexual relationship is formed.

Also, in some circumstances, the development of a personal relationship between employees where there is a reporting line or a decision making role may be inappropriate unless appropriate steps are taken.

Where a personal relationship occurs in situations covered by this policy, employees must take steps to manage any conflict of interest or imbalance of power, including, where necessary, declaring any such relationship, or potential relationship, to Police.

Where appropriate, Police will take all reasonably practicable steps to manage any conflict of interest or imbalance of power that may arise. Where a personal relationship already exists, Police employees will need to either avoid or take steps to manage any direct dealings with that person in a professional capacity where a conflict of interest or power imbalance may arise.

Breach of policy

Any breach of this policy may be a breach of the New Zealand Police Code of Conduct, and may result in disciplinary action, including dismissal.

Definitions

For the purposes of this policy, the following definitions apply:

*Personal relationship***:** A personal relationship may include (but is not limited to) a sexual relationship; conduct or contact that has an intimate as opposed to professional intention; family members.

Professional relationship: A professional relationship is where the relationship has arisen out of the employee's work duties. This includes, but is not necessarily limited to, a relationship between two Police employees, or a Police employee and members of the public, or a Police employee and staff of external agencies or contractors.

Conflict of interest: A conflict of interest can be described as a situation in which a person has a private or personal interest which could or could reasonably be perceived to influence the objective exercise of their official duties as an employee.

Reporting line relationship: these include situations where the relationship is between employees in a line management relationship which does not involve a direct reporting relationship (e.g. a relationship between an employee and their manager's manager).

External relationships – employee's obligations

Police recognise that the formation of a personal relationship, and in particular, a sexual relationship with the following groups of people whilst they interact with the Police employee in a professional capacity, creates the greatest risk of a conflict of interest or imbalance of power arising and are therefore considered to be unethical.

Police employees must avoid entering into a personal relationship with the following groups of people whilst they are in a professional relationship and during any subsequent period of time during which an imbalance of power or conflict of interest could be perceived to exist:

- complainants when the employee is dealing with a complainant in a professional capacity and the power relationship could be perceived to influence decision making
- offenders when they have current charges and/or a known criminal history
- witnesses and their family members involved in a matter the employee is dealing with in a professional capacity where the power relationship could be perceived to influence decision making
- informants
- vulnerable persons where a duty of care exists
- any person in custody.

(This list is not exhaustive but is illustrative only)

In addition, there will be other circumstances where an employee contemplates entering into a personal relationship with an external person they are having professional dealing with, or where an employee is already in a personal relationship and may need to interact with that person in a professional capacity. This would include interactions with family, friends and associates in a professional capacity. These situations may also give rise to a conflict of interest.

If an employee intends to enter into a personal relationship of this nature or is uncertain as to whether the relationship is covered by this section, they must declare it to their local Human Resources Manager prior to the commencement of the relationship.

It is inappropriate to terminate a professional relationship in order to develop a personal relationship except in cases where the relationship is reported to Police and appropriate safeguards are put in place to remove the conflict of interest or power imbalance.

External relationships – employer's obligations

Where a relationship is raised with the Human Resources Manager, the manager must then assess whether or not steps can be taken to put in place safeguards to manage any conflict of interest or power imbalance. This could include removing the employee from any professional involvement with the person. Where appropriate all reasonably practicable steps will be taken to allow the relationship to continue.

Some relationships will, however, always remain unethical due to their nature as no appropriate safeguards can be put in place. All relationships will be considered on a case by case basis, taking into account all of the circumstances. Before a decision is made the employer will consult with the employee concerned.

Internal relationships – employee's obligations

Police accept that relationships between employees exist and will continue to develop. This is only an issue where there may be (or may be reasonably be perceived to be) a conflict of interest or power imbalance.

Where an employee has a personal relationship with anyone that they have a professional relationship with, which may lead to the perception of a conflict of interest or power imbalance, they must:

- take steps themselves to manage any conflict of interest or imbalance of power, or
- discuss the matter with their supervisor or Human Resources Manager.

This policy does not apply to professional interactions between two colleagues of the same level or rank who are in a sexual relationship as it is unlikely a conflict of interest or power imbalance will arise.

Some internal personal relationships will always be unethical, for example:

- where a direct reporting line relationship develops or exists between the people and that has not been reported
- between instructors and recruits, and instructors and advanced trainees while attending training or undergoing assessment.

These relationships are to be avoided. If an employee intends to enter into a personal relationship of this nature, they must first declare it to their local Human Resources Manager.

Internal relationships – employer's obligations

Where a relationship is declared, the Human Resources Manager must then assess whether or not steps can be taken to put in place safeguards to manage any conflict of interest or power imbalance. Where appropriate all reasonably practicable steps will be taken to allow the relationship to continue.

All relationships will be considered on a case by case basis, taking into account all of the circumstances. Before a decision is made the employer will consult with the employee concerned.

Transitional provisions

Where an employee is in both a personal and professional relationship (refer to Types of relationships and Management of relationships) at the time that this policy comes into effect, consideration will be given to the appropriate manner in which to manage the professional relationship. This could include removal from an enquiry or operation, or a change in reporting lines, for example. An employee will not be required to end a pre-existing personal relationship pursuant to this policy.

An employee in an external relationship needing to be declared at the time this policy is introduced must:

- report that relationship to either their supervisor or the appropriate Human Resources Manager
- take steps themselves to manage any conflict of interest or imbalance of power, and
- discuss any issues relating to the management of conflicts of interest or imbalance of power with their supervisor or Human Resources Manager.

Where it is appropriate to put in place safeguards, relevant considerations to be taken into account in assessing the best possible way of managing a pre-existing personal relationship include:

- the nature of the relationship at the time the policy comes into effect
- whether the relationship is one that is to be avoided under this policy
- the extent to which there is potential for a conflict of interest (actual or perceived) or imbalance of power to arise, and
- the safeguards (if any) that can be put in place to manage any conflict of interest or imbalance of power.

Any other relationship does not need to be declared, unless a conflict of interest may arise.

2. Extract from the Acceptable Use of Technology, Resources and Information Policy

Purpose

Police technology, equipment and information repositories are provided and maintained for the purpose of conducting Police business. This chapter defines "acceptable use" of Police technology and resources, whether it is for Police business or for personal purposes.

Application

All users of Police telephones, computer systems and office equipment (employees, contractors and other authorised third party users) must comply with this chapter, and take any other necessary steps to ensure that the resources are not misused in any way that would jeopardise their operation or availability, or expose Police to risk.

Managers must ensure that new Police employees, newly engaged contractors or other third party users are made aware of this and related instructions. Copies should be provided as part of the induction process, and consideration given to requiring a signed acknowledgement of receipt.

Risks for users

The privilege of limited personal or private use will be withdrawn if abuses are detected. Unauthorised, inappropriate or excessive personal use of Police resources could also result in disciplinary action (including dismissal) for employees, or contractual penalty or civil liability for non-employees who have been given access.

Prosecution is possible if misuse - particularly if it involves use of Police systems for unlawful or objectionable purposes as defined in this policy - amounts to a criminal offence.

Conditions of use of Police computer systems

Authorisation of use by any person of Police computers and ancillary technology is conditional on compliance with this and related policies, and is on the basis that misuse may be subject to disciplinary action or prosecution.

Users of the Police computer (Enterprise) system are presented with a warning screen at the commencement of the log on process, and are required to click an on-screen button before they can proceed. The log on banner looks like this:

Use is logged, recorded and reviewed

Police logs access to computer systems and applications, and records and may review the uses to which its technology and resources are put.

If it becomes necessary to examine non-business or private communications as part of investigations, for example into suspected disciplinary or criminal offences, Police will follow established protocols for authorising recovery of data and the use of forensic tools - refer to "Protocols for ICT security investigations".

Permitted use of technology and equipment

Use for Police purposes

Technology, resources and information are provided for the conduct of Police business. It is usually very clear what is done in the course of employment, and what is not. Police employment policies, instructions and the Code of Conduct give further guidance.

Use of Police technology, resources and information for Police business purposes is approved, subject to statute, this and other policies, and specific management direction.

Limited personal use of technology and equipment

Users may make limited personal use, at work, of Police technology and equipment, subject to their meeting responsibilities defined in this policy and their acceptance that personal use is not a right, but a privilege which will be revoked if abused.

Reporting misuse of technology and equipment: requirement to report

All users of Police technology and resources must report instances, other than trivial, of prohibited use ... or damage to or loss of equipment or information.

Prohibited personal use of Police information

Business versus personal use of information

Authorised users of Police ICT systems have access to official and personal information in databases and applications designed and intended only for Police business purposes.

The Privacy Act 1993, other statutes and policy (refer to "Security of information") effectively prohibit the use and disclosure of official information for private purposes. The consequences of inappropriate access and use are potentially serious for both Police and user.

Conflicts of interest

Police employees may on occasion find themselves privy to information that, although it is legitimately obtained for Police business purposes, may set up a conflict of interest, or create tension between Police duties and personal obligations.

Police employees, and others with authorised access to Police information, **must** declare such personal or private interest in official matters to management and accept and abide by decisions that they should have no further involvement in the matter, and not receive or seek out any further information about it.

Examples of inappropriate access

Irrespective of the 24 hour statutory role of Police constables, it is inappropriate for Police information systems to be accessed for private purposes. These are examples of inappropriate access (non-exhaustive list):

- checking NIA for criminal histories of acquaintances, or ascertaining the name and address of a vehicle owner
- using TESA to obtain a telephone number or address not recoverable from public directories
- using CARD to obtain information about occurrences, not available in the public domain
- obtaining information about identities and charges in prosecutions prior to court appearances, or which become subject to suppression orders
- providing "unofficial" assistance or advice, based on protected Police-sourced information, to family or friends
- "celebrity surfing" i.e. seeking out information about public figures
- merely satisfying personal curiosity about any matter.

Prohibitions on access

Users must not access or attempt to access; intercept; pass on; copy; or use in any manner any information held in or derived from Police information systems unless it is for official Police business purposes.

This prohibition particularly applies, but is not restricted to information held in or on:

- National Intelligence Application (NIA)
- Telephone Emergency Subscriber Access (TESA)
- Communication and Resource Deployment system (CARD)
- PeopleSoft