Acceptable use of information and ICT

Table of Contents

You must not use Police technology, information or other resources for unethical or inappropriate purposes or against Police policy, whether that is inadvertent or intentional.

If you do discover that you have made an error of inappropriate accessing, using or procuring information or technology you should notify the appropriate managers and/or your manager as soon as possible.

You must not (non-exhaustive list):

- access, or attempt to access, use or disclose, any official or personal information unless it is for official Police business purposes, duties and responsibilities
- use Police equipment to install, copy, distribute, use or otherwise infringe copyright
- intentionally download, hold, transmit, view or present to any other person any objectionable or offensive material unless required for an authorised Police operation
- tamper with or attempt to circumventor any system or security measures
- download or install software without proper approvals
- procure software, hardware and IT-related services on behalf of Police without authorisation.

In some circumstances, use that is otherwise inappropriate may be approved by a member of the Police Executive or a Director if it is for official Police business purposes. The scope and approval must be in writing. Approval from the Chief Information Officer will also be needed if the intended use could adversely affect ICT systems or services.

Use of information

Irrespective of the 24 hour statutory role of Police constables, it is inappropriate for official Police information to be used for private purposes. Examples of inappropriate access (non-exhaustive list) include:

- checking NIA for details of neighbours, acquaintances or celebrities
- obtaining information about identities and charges in prosecutions prior to court appearances or under suppression orders
- using TESA to obtain a telephone number or address not recoverable from public directories
- providing assistance or advice, based on protected Police-sourced information, to family or friends.

The Privacy Act and other statutes prohibit the access, use and disclosure of official information for private purposes. The consequences of inappropriate access and use are potentially serious for both Police and user. Offences related to unauthorised possession or disclosure of information include:

Statute	**Offence**
Section 20A of the Summary Offences Act 1981	Communicating information where the disclosure may endanger safety or prejudice law enforcement.
Section 17 of the Criminal Records (Clean Slate) Act 2004	Criminal histories are protected from disclosure outside Police except for specified purposes.
Sections 105A and 105B of the Crimes Act 1961	Corrupt disclosure or use of official or personal information that has been obtained in an official capacity.
Section 50 of the Policing Act 2008	Possessing Police property without lawful authority or reasonable excuse. Police property includes Police information.

Personal use of ICT

Limited personal use of Police technology, equipment, supplies and other resources is permitted, but it must at all times:

- be consistent with Police values and standards of behaviour expected of an employee
- be consistent with the terms of authorisation and direction of management
- be kept to a minimum so that your official duties are not compromised
- not incur direct cost (other than trivial) for Police or interfere with the use of the resources by others (you may need to reimburse Police for the cost of personal use if that cost or consumption is more than trivial.)

You can, for example:

- email friends from your work address
- check news stories
- look up public addresses and phone numbers.

You should not, for example:

- view, download or otherwise handle potentially offensive content
- post on social media as a Police employee unless authorised as part of your role
- conduct non-Police business
- gamble
- waste time browsing the internet
- make lengthy or long-distance personal phone calls or otherwise use resources for non-Police business activity to the point that performance or availability of services could be affected.

If you are unsure whether it is appropriate, consider Code of Conduct and the SELF CHECK (stand up to Scrutiny; Ensure compliance; Lawful; and Fair).

Printed on : 09/06/2022