Information security: 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 applicable Police teams and/or your manager as soon as possible.

You must not (non-exhaustive list):

- collect, access, or attempt to access, use or disclose, any official or personal information and other content (e.g. photographs) unless it is for official Police business purposes, duties and responsibilities and in line with Police doctrine
- 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 or IT-related services on behalf of Police without authorisation
- enter or upload Police official information or personal information in Police custody to any website or service that has not been formally approved for Police use. **Note:** this includes Artificial intelligence services.

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 Police ICT systems or services.

Use of information

Official Police information - including but not limited to NIA data - must never be used for private purposes. Examples of inappropriate access (non-exhaustive list) include, without business justification or approval:

- 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
- sharing photos on a Police issued device or USB with a non-Police authorised device.

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. Examples of 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.**Note:** you may have 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 as long as it is clear that the interaction is not official
- 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.

Use of USBs

Personal USBs can be used for policing purposes but must only be used to transfer information to a Police computer. The transferred data must then be deleted off of the personal USB. All other use of personal USB devices is not authorised.

When required to use or examine USBs provided by others e.g., members of the public, you must seek support and advice from your regional digital first responders before attempting to access the storage device. See USB device reminder for further information.

If you are unsure whether it is appropriate, consider Code of Conduct and the SELF CHECK.