Police
Instructions

Social Networking, Open Source Information and Online Practitioner

Table of Contents

Table of Contents 3

Executive summary 4

- Overview 4
- Principles 4
- Responsible use of online personas 4
- The Internet 4
- Acceptable use of technology 5
- Using social media sites 5
- s.6(c) OIA 5
- Definitions 5
- Police contacts 6

Online personas 8

- Features of an online persona 8
- Registration 8
- Authorisation 8
- s.6(c) OIA 9
- The persona pool 9
- s.6(c) OIA 9
- Persona deregistration 10
- Consent 10
- Personal personas 10

Open Source Information and Online Practitioner 11

- Role 1: Overt Online 11
- Role 2: Discreet Online Researcher 11
- Role 3: Discreet Online Persona 12
- Role 4: Discreet Online Controlled Operations 12
- Role 5: Discreet Online Specialist 12

Equipment 14

- s.6(c) OIA 14
- s.6(c) OIA 14
- Cellular/mobile phone verification 14
- Home or personal device 14

Evidence capture 16

- Methodology 16
- Social Networking chapter 16
- Disclosure 17

Organisational risk 18

- Disclosure of online investigations methodology 18
- s.6(c) OIA 18
- Legislation 18
- Committing offences 18

Executive summary

Due to the rapid pace of technological change, increasing connectivity and the popularity of social media, the internet has become a vast source of evidence and information.

Almost all investigations involve a component of technology, whether it is in the process of gathering information (open source / social media), during the commission of the offence (direct electronic evidence), concealing the proceeds of crime through the banking system, crypto currencies or indirect electronic evidence (e.g. social media posts).

Police must be aware of these key, critical points:

- Police employees are accountable for how they utilise the internet not only for public relations, but also as a source of information and evidence.
- No online practitioner activities should be conducted or authorised outside of the Police Manual mandated policy and procedures.

Overview

This chapter aims to ensure lawful, ethical, and reasonable use that is consistent and proportionate to operational requirements.

Principles

The key principles of this chapter are:

- s.6(c) OIA exemplify Police values and must be ethical and lawful at all times.
- No Police employee must obtain, create, or otherwise use an online persona without the approval of the appropriate authority.
- All online profiles must be registered in accordance with this chapter to ensure national consistency, organisational accountability and to enable national and international deconfliction.
- The safety and welfare of staff involved with online investigations is of paramount importance. It is essential that all online investigations are able to withstand stringent scrutiny.

Responsible use of online personas

Employees are responsible for ensuring that all online investigation activities are conducted in accordance with this chapter. Operating and managing an online persona outside of the directions of the manual, may lead to action under the Police 'Code of Conduct'.

The Internet

The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve several billion users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW), the infrastructure to support email, and peer-to-peer networks.

The Internet has no centralised governance in either technological implementation or policies for access and usage; each constituent network sets its own policies. Only the Internet Protocol address framework and the Domain Name System are managed by a maintainer organisation, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardisation of the core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a non-profit organisation of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

Acceptable use of technology

All instructions outlined in this chapter are to be implemented in conjunction with 'Information management, privacy and assurance' chapter of the Police Manual.

Using social media sites

All instructions outlined in this chapter are to be implemented in conjunction with the 'Social media policy' chapter of the Police Manual.

s.6(c) OIA

[redacted]

Definitions

This table details definitions of terms relevant to this chapter.

Term	Definition
s.6(c) OIA [redacted]	[redacted]
Cybercrime	‘Cybercrime’ is defined as a criminal act that can only be committed through the use of ICT or the Internet and where the computer or network is the target of the offence. This is regardless of what the criminal goal is - whether political, financial gain, espionage or any other reason. Examples of this would be malicious software, network intrusion, denial of service attacks and phishing.
Cyber-enabled crime	‘Cyber-enabled crime’ is any criminal act that could be committed without ICT or the Internet, but is assisted, facilitated or escalated in scale by the use of technology. This includes a vast amount of serious and organised crime, such as cyber-enabled fraud or the distribution of child exploitation material.
Cyber safety	‘Cyber safety’ is the safe and responsible use of Information and Communication Technologies (ICT).
Cyber security	‘Cyber security’ is the application of protocols, devices or software to secure data in storage or transit from attack, unauthorised access, deletion or modification.
Online persona	‘Online persona’ is an assumed identity or fabricated identity that has been created to conceal the true identity of the user e.g. a false email address or Facebook profile.
Online practitioner	‘Online practitioner’ refers to an investigator who lawfully and ethically utilises the Internet as an investigative tool.
Open Source Intelligence (OSINT)	‘Open Source Intelligence (OSINT)’ is information collected from publicly available sources (as opposed to covert or clandestine sources).
Registered persona	‘Registered persona’ is an approved police persona that has been registered and is operated in accordance with this chapter.
Social networking	‘Social networking’ is the creation and maintenance of personal and business relationships online.

Police contacts

This table details the relevant Police contacts.

Cybercrime Unit	[redacted]	[redacted]
Digital Forensic Units	[redacted]	[redacted]
OCEANZ	[redacted]	[redacted]
s.6(c) OIA [redacted]	[redacted]	[redacted]

Online personas

It is becoming increasingly necessary for staff to engage with targets or POI's on social media or other online forums using an assumed identity or persona.

This may be for the purpose of gathering more in-depth information about persons or events, or to gather evidence about criminal offending.

When considering whether to utilise an online persona, an appreciation should be conducted regarding what the aims of the deployment are, whether its use is lawful, reasonable, proportionate and necessary in the circumstances. This should be considered alongside legislative constraints and organisational risk.

Features of an online persona

An online persona:

- is created, maintained and utilised for legitimate overt or covert policing activities
- can be an individual, a business or any other entity
- may have no connection to the identity/name of any Police employee
- s.6(c) OIA
- is only utilised for the specific objectives of its deployment.

Registration

s.6(c) OIA

The registration of online personas is essential to ensure national consistency, organisational accountability, protect the safety and welfare of staff and to enable national and international deconfliction where appropriate. A database will ensure that existing profiles can be assessed and deployed operationally for controlled operations, e.g. if it is a member of a specific group of Police interest.

The registration of any online persona deployed for the purpose of online investigations will be conducted prior to any investigative activity utilising the persona. Registration can be accomplished by contacting the s.6(c) OIA PNHQ for a registration form.

s.6(c) OIA

Registering officers will become the 'owner' of that profile. Owners will be permitted access to their registered profiles in the register at any time to ensure that they are regularly updated and current.

Authorisation

The completed registration form must be approved by a supervisor or manager in accordance with the relevant level of authorisation for each role as outlined in this table.

Role	Level of Authorisation
Role 1: Overt Online	Self-approved
Role 2: Discreet Online Researcher	Sergeant, **equivalent** or above
Role 3: Discreet Online Persona	Senior Sergeant, **equivalent** or above
Role 4: Discreet Online Controlled Operations	District Crime Services Manager, **equivalent** or above
Role 5: Discreet Online Specialist	Manager of the High Tech Crime Group or the Manager of the Covert Operations Group or above

When authorising the deployment of an online persona the authorising officer must consider whether its use is **lawful**, reasonable, proportionate and necessary in the circumstances. An organisational risk assessment must accompany the registration request.

s.6(c) OIA

[redacted]

[redacted]

[redacted]

The persona pool

s.6(c) OIA, the Cybercrime Unit can be contacted and the database searched to assess if a suitable online persona is registered and available for redeployment.

The redeployment of a persona will only be permitted following a comprehensive risk assessment and with the authority and assistance of the owner.

s.6(c) OIA

[redacted]

[redacted]

Persona deregistration

In order to maintain an accurate up to date database, it is essential to update personas should they become inactive, compromised, or retired.

s.6(c) OIA

Consent

On occasions it may be assessed that the most effective way to extract online information or evidence is to 'take over' the existing account of a victim, witness or co-offender.

This can be an effective investigative tool to progress an investigation however, a comprehensive risk assessment and appreciation is required to mitigate risk to the victim, witness or co-offender and Police.

All personas that are adopted under 'consent' are to be registered as outlined in this chapter. The profile registration form will be endorsed 'consent' during the registration process.

Upon completion of the period of consent, it is essential that the profile is retired when no longer required.

Authorisation to assume a victim, witness or co-offender's profile can only be granted by an Inspector or above and a consent form completed. Consent forms can be located here.

Personal personas

No personal personas (disused, obsolete or otherwise) associated with past or current police employees or associates will be utilised for any roles outlined in this chapter unless by consent or required by unique operational circumstances.

Open Source Information and Online Practitioner

It is recognised that most investigations into Crimes Act offences now have an online component to them. Evidence or information posted on Social Networking sites or other forums can create or direct phases of investigation and assist with developing target profiles, associates and attribution.

Police have adopted a framework which defines how information and evidence is identified from online sources and by whom. These five roles each outline specific expectations and restrictions:

- Overt Online
- Discreet Online Researcher
- Discreet Online Persona
- Discreet Online Controlled Operations
- Discreet Online Specialist

Role 1: Overt Online

This role describes the knowledge and skills required to conduct general queries overtly online. The purpose of this role is to facilitate police activities on the internet.

This role describes the online capabilities required for individuals whose duties require performing activities and engaging online as a police employee, e.g. public affairs, community policing teams or prevention initiatives.

An employee performing this role **does not** utilise an online persona (assumed identity).

For further instruction on using social media for community engagement and guidance on private use, see ‘Social media policy’.

Role 2: Discreet Online Researcher

This role describes the knowledge and skills required to conduct discreet research using the internet.

A risk assessment for discreet research will be completed and authorised by a supervisor of at least the rank of Sergeant.

Practitioners will have successfully completed training to **Level 1** of the National Cybercrime Training Programme and will be fully conversant with legislative and policy guidelines and restrictions.

- An employee performing this role may utilise an overt identity if risk of discovery has been assessed as minimal and/or insignificant.
- An employee performing this role may utilise a registered assumed identity if risk of discovery has been assessed as possible and/or likely.
- An employee performing this role remains passive s.6(c) OIA
- A Discreet Online Researcher s.6(c) OIA

Role 3: Discreet Online Persona

This role describes the knowledge and skills required to apply online capabilities to investigate crimes using registered personas.

A risk assessment for deployment of the registered persona will be completed and authorised by a supervisor of at least the rank of Senior Sergeant.

Practitioners will have successfully completed the online elements of**Level 1 and 2** of the National Cybercrime Training Programme and will be fully conversant with legislative and policy guidelines and restrictions.

- At the Senior Sergeant's discretion, an employee performing this role may utilise a registered assumed identity.
- s.6(c) OIA.
- A Discreet Online Persona maintains s.6(c) OIA
- s.6(c) OIA

Role 4: Discreet Online Controlled Operations

This role describes the knowledge and skills required to support and contribute to workgroups in specialised areas, s.6(c) OIA

A risk assessment for deployment of the registered persona will be completed and authorised by at least a District Crime Service Manager, Manager of the Covert Operations Group or above.

Practitioners will have successfully completed the online elements of**Level 1 and 2** of the National Cybercrime Training Programme and will be fully conversant with legislative and policy guidelines and restrictions.

- An employee performing this role will utilise a registered assumed identity
- s.6(c) OIA
- An employee performing this role will be s.6(c) OIA as outlined in the 'Equipment' section of this chapter.
- The role of Discreet Online Controlled Operations s.6(c) OIA

Role 5: Discreet Online Specialist

This role describes the knowledge and skills required by individuals who are targeting offenders with s.6(c) OIA The Discreet Online Specialist will possess high level skills and knowledge of the investigation intricacies to ensure credibility is maintained s.6(c) OIA

A risk assessment for deployment of the registered persona will be completed and authorised by at least the Manager: National High Tech Crime Group or the Manager: Covert Operations Group or above.

Practitioners will have successfully completed the online elements of**Level 1 and 2** of the National Cybercrime Training Programme as well as additional specialist training provided by the Cybercrime Unit. Practitioners will be fully conversant with legislative and policy guidelines and restrictions.

- An employee performing this role will utilise a registered assumed identity.
- s.6(c) OIA
- An employee performing this role will be s.6(c) OIA as outlined in the ‘Equipment’ section of this chapter.
- A Discreet Online Specialist s.6(c) OIA

Equipment

Careful consideration needs to be taken to ensure that the right equipment is being utilised when operating an online persona.

s.6(c) OIA

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

Cellular/mobile phone verification

When registering your online persona with various applications, you may be required to supply a cellular/mobile phone number to verify or activate the account. You should assess the objectives of the online persona created and evaluate if you wish to supply a non-attributable cellular/mobile number to the service.

In exceptional circumstances you may wish to consider the cash purchase and activation of a pay as you go cellular/mobile phone.

Home or personal device

A personal computer system or device must **not** be utilised for any roles outline in this chapter.

Evidence capture

Methodology

It is essential that online information or investigation activity can be recorded, to prove how the information or evidence was obtained. Methods of documenting online investigative processes can include, but is not limited to:

- comprehensive notebook entries
- screen prints
- photographing or videoing the screen interactions
- third party software designed to capture data.

Advice should be sought from the Cybercrime Unit regarding evidence capture methods.

Social Networking chapter

It may be possible to recover information or evidence of your interaction retrospectively. Refer to the '[Social Networking Guide](#)' (see PDF below) for further information. Note that the Guide is currently under review and will be replaced by a chapter in the Police Manual.

-

NZ Police Online Investigation Guide (OIG) v2.06 **3.61 MB**

This guide has been designed to assist investigators in identifying information that can be obtained from various social media and online companies. Social networking is the creation and maintenance of personal and business relationships, especially online. While numerous social media sites are covered in this guide, other online sites are also covered to ensure investigators are aware of the information they can obtain.

Updates in Version 2.04

- Uber content added. Google content updated.

Updates in Version 2.03

- PaySafe content added.

Updates in Version 2.02

- Tinder updated. Omegle content added.

Updates in Version 2.01

- Facebook details amended.

Disclosure

For prosecutions Police must comply with the Criminal Disclosure Act 2008. It is essential that a detailed record of any online activities is fully documented so that obligations under the Act can be met.

Organisational risk

Although some risk-taking is inevitable in the execution and pursuit of our objectives, being risk aware means that we not only actively manage potential problems, but also identify potential opportunities. To manage risk, we need to identify and evaluate the risks we face as an organisation

Disclosure of online investigations methodology

Every effort should be implemented to safeguard the disclosure of the Police methodology and techniques when conducting online investigations. s.6(c) OIA [redacted]

The disclosure of a Police persona and its use in a covert operation is likely to cause significant media attention and may impact on the organisations reputation.

s.6(c) OIA [redacted]

[redacted]

[redacted]

Legislation

As we utilise the internet as a source of information and evidence we need to comply with New Zealand Legislation. The New Zealand Bill of Rights Act 1990, the Privacy Act 2020, the Crimes Act 1961 and the Search and Surveillance Act 2012 all have sections that limit what Police can lawfully do.

There is a fine line between what is in the public domain and what is not and therefore Police need to mitigate any organisation risk by evaluating legislative implications and ethical obligations.

Police may be required to justify that their actions were lawful, ethical, reasonable, consistent and proportionate to operational requirements.

Committing offences

Current legislation does not permit police to commit any offence for the purpose of progressing with an investigation other than outlined in the Misuse of Drugs Act 1975.

Printed on : 09/11/2021

Printed from : https://tenone.police.govt.nz/pi/social-networking-open-source-information-and-online-practitioner

Table of Contents

Table of Contents 2

Policy statement and principles 3

- What 3
- Why 3
- How 3

Overview 4

- Key operating principles 4
- Responsible use of online personas 4
- Acceptable use of technology 4
- Account takeover 4
- s.6(c) OIA 4
- Definitions 4
- Police contacts 5

Online personas 6

- Features of an online persona 6
- Registration 6
- Authorisation 6
- s.6(c) OIA 7
- s.6(c) OIA 7
- Persona deregistration 7
- Consent takeover of accounts 7
- Personal personas 8

Open-Source Information and Online Practitioner 9

- Role 1: Overt Online 9
- Role 2: Discreet Online Passive Operations 9
- Role 3: Discreet Online Active Operations 9
- Role 4: Discreet Online Controlled Operations 10
- Role 5: Discreet Online Advanced Operations 10

Equipment 11

- s.6(c) OIA 11
- [redacted] 11
- Accounts on social media and other services 11
- Cellular/mobile phone verification 11
- Home or personal device 11

Evidence capture 12

- Methodology 12
- Social Networking chapter 12
- Disclosure 12

Organisational risk 13

- Reducing organisational risk 13
- Disclosure of online investigations methodology 13
- [redacted] s.6(c) OIA 13
- Legislation 13
- Committing offences 13

Policy statement and principles

What

The ‘Social Networking, Open-Source Information and Online Practitioner’ chapter provides guidance to Police employees about the lawful, ethical, and reasonable use of gathering information (open-source/social media), during the commission of the offence (direct electronic evidence), concealing the proceeds of crime through the banking system, cryptocurrencies or indirect electronic evidence (e.g., social media posts).

Why

The rapid pace of technological change with the internet, increasing connectivity, and the popularity of social media has provided a vast source of evidence and information for resolving crime.

How

Police will:

- be accountable with individual responsibility under the ‘Code of Conduct’ for how it utilises the internet not only for public relations, but also as a source of information and evidence
- not conduct or authorise online practitioner activities outside of the Police Manual mandated policy and procedures
- comply with legislation and the key operating principles outlined in this chapter.

Overview

This chapter aims to ensure lawful, ethical, and reasonable use of gathering information (open-source/social media) that is consistent and proportionate to operational requirements.

Key operating principles

The key principles under which Police must operate include that:

- s.6(c) OIA [redacted] exemplify Police values and must be ethical and lawful at all times
- the safety and welfare of employees involved with online investigations is of paramount importance (it is essential that all online investigations are able to withstand scrutiny)
- Police employees must obtain approval of the appropriate authority before acquiring, creating, or otherwise using an online persona
- Police employees may monitor and use publicly accessible social media information to fulfil Police's functions under section 9 of the Policing Act 2008
- Police employees must first have the approval of their supervisor to monitor social media networks, (complete the'Request for Restricted Internet Access' form, go to ICT Portal, then search 'Restricted internet access' for accessing social media networks on enterprise devices)
- all online profiles must be registered in accordance with this chapter to ensure national consistency, organisational accountability, and to enable national and international deconfliction
- the Police Manual chapter 'Acceptable Use of information and ICT' applies to information collected
- all information collected must be stored securely and protected against loss, unauthorised access, use, modification, or unauthorised disclosure
- information collected which is no longer required for intelligence, evidentiary, or investigatory purposes must be destroyed in accordance with provisions under the Public Records Act 2005
- sharing of information collected must abide by the principles of the Privacy Act 2020
- day-to-day monitoring of social media networks must be done through a designated Police account using approved social monitoring software
- the accounts used for monitoring publicly accessible social media networks must**not** be used for external communications by Police to the public, i.e., 'to tweet'.
- Police use of social media for external communication of material to the public for community engagement or private use is covered by the 'Social media policy' chapter
- Police employees can only operate at a particular Online Practitioner level (2-5) when trained, certified, and appropriately supervised.

Responsible use of online personas

Employees are responsible for ensuring that all online investigation and intelligence gathering activities are conducted in accordance with this chapter. Operating and managing an online persona outside of the directions of the manual, may lead to action under the Police 'Code of Conduct'.

Acceptable use of technology

All instructions outlined in this chapter are to be implemented in conjunction with 'Acceptable use of information and ICT' chapter of the Police Manual.

Account takeover

All instructions in this chapter must be implemented in conjunction with the 'Account takeover policy' chapter of the Police Manual

s.6(c) OIA [redacted]

[redacted]

Definitions

This table details definitions of terms relevant to this chapter.

Term	Definition
s.6(c) OIA [redacted]	[redacted]
Cyber-dependent crime	‘Cyber-dependent crime’ is defined as a criminal act that can only be committed through the use of ICT or the internet and where the computer or network is the target of the offence. This is regardless of what the criminal goal is - whether political, financial gain, espionage, or any other reason. Examples of this would be malicious software, network intrusion, denial of service attacks, and phishing.
Cyber-enabled crime	‘Cyber-enabled crime’ is any criminal act that could be committed without ICT or the internet, but is assisted, facilitated, or escalated in scale by the use of technology. This includes a vast amount of serious and organised crime, such as cyber-enabled fraud or the distribution of child exploitation material.
Cyber safety	‘Cyber safety’ is the safe and responsible use of Information and Communication Technologies (ICT).
Cyber security	‘Cyber security’ is the application of protocols, devices or software to secure data in storage or transit from attack, unauthorised access, deletion or modification.
Online persona	‘Online persona’ is an assumed identity or fabricated identity that has been created to conceal the true identity of the user e.g., a false email address or Facebook profile.
Online practitioner	‘Online practitioner’ refers to an investigator who lawfully and ethically utilises the internet as an investigative tool.
Open-Source Intelligence (OSINT)	‘Open-Source Intelligence (OSINT)’ is information collected from publicly available sources (as opposed to covert or clandestine sources) and processed into actionable insights
Registered persona	‘Registered persona’ is an approved police persona that has been registered and is operated in accordance with this chapter.
Social networking	‘Social networking’ is the creation and maintenance of personal and business relationships online.

Police contacts

This table details the relevant Police contacts.

Cybercrime Unit	[redacted]	[redacted]
Digital Forensic Units	[redacted]	[redacted]
Covert Online Team (including OCEANZ)	[redacted]	[redacted]
s.6(c) OIA [redacted]	[redacted]	s.6(c) OIA [redacted]
OSINT Team	[redacted]	Nil ext.

Online personas

It is becoming increasingly necessary for trained staff to conduct targeted research of social media or other online forums, including, where appropriate, engagement with targets or POI's using an assumed identity or persona.

This may be for the purpose of gathering more in-depth information about persons or events, or to gather evidence about criminal offending.

When considering whether to utilise an online persona, an appreciation should be conducted regarding what the aims of the deployment are, whether its use is lawful, reasonable, proportionate, and necessary in the circumstances. This should be considered alongside legislative constraints and organisational risk.

Features of an online persona

An online persona:

- is created, maintained, and utilised for legitimate overt or covert policing activities
- can be an individual, a business or any other entity
- may have no connection to the identity/name of any Police employee
s.6(c) OIA
- is only utilised for the specific objectives of its deployment.

Registration

s.6(c) OIA

The registration of online personas is essential to ensure national consistency, organisational accountability, protect the safety and welfare of staff, and to enable national and international deconfliction where appropriate. A database will ensure that existing profiles can be assessed and deployed operationally for controlled operations, e.g., if it is a member of a specific group of Police interest.

The registration of any online persona deployed for the purpose of online investigations will be conducted prior to any investigative activity utilising the persona. Registration can be accomplished by contacting the s.6(c) OIA

s.6(c) OIA

Registering officers will become the 'owner' of that profile. Owners will be permitted access to their registered profiles in the register at any time to ensure that they are regularly updated and current.

s.6(c) OIA

Authorisation

A completed online persona registration form must be approved by a supervisor or manager in accordance with the relevant level of authorisation for each role as outlined in this table. This is in addition to registering the online persona.

Role	Level of Authorisation
Role 1: Overt Online	Self-approved
Role 2: Discreet Online Passive Operations	Sergeant, **equivalent** or above
Role 3: Discreet Online Active Operations	Senior Sergeant, **equivalent** or above
Role 4: Discreet Online Controlled Operations	Manager of the High Tech Crime Group s.6(c) OIA or above National Criminal Investigation Group, as well as the National Security Group.
Role 5: Discreet Online Advanced Operations	Director National Criminal Investigation Group, or National Security Group.

When authorising the deployment of an online persona the authorising officer must consider whether its use is**lawful**, reasonable, proportionate, and necessary in the circumstances. An organisational risk assessment must accompany the registration request. Supervisors should be aware of how the online persona is being deployed and have oversight of any groups it is in.

s.6(c) OIA

[redacted]

Deconfliction

The potential for anonymity of the internet provides many challenges as law enforcement agencies (LEA) around the world operate in the online environment to identify, investigate, and prosecute online criminal activities. In order to ensure that LEA are not targeting each other, there has to be a process to eliminate conflict.

s.6(c) OIA will have access to all registered online personas and will be the contact point for deconfliction enquiries.

Persona deregistration

In order to maintain an accurate up to date database, it is essential to update personas should they become inactive, compromised, or retired.

When a profile is deregistered by its owner, it will be assessed by s.6(c) OIA and consideration will only be given for reallocation or redeployment once a current organisational risk assessment has been conducted and considered.

Consent takeover of accounts

On occasions it may be assessed that the most effective way to extract online information or evidence is to 'take over' the existing account of a victim, witness or co-offender.

An account takeover differs from the authority to download an account (for example a Google takeout), and is covered by the'Account takeover policy'. Where an investigative opportunity exists to take over an account, consideration should be taken to engage a specialist team such as the Covert Online Team (COLT) to undertake a covert online engagement.

A comprehensive risk assessment and appreciation is required to mitigate risk to the victim, witness or co-offender and Police.

All personas that are adopted by Police under 'consent' are to be registered as outlined in this chapter. The profile registration form will be endorsed 'consent' during the registration process.

Upon completion of the period of consent, it is essential that the profile is retired when no longer required.

Authorisation to assume a victim, witness, or co-offender’s profile can only be granted by an Inspector or above and a consent form completed. Both forms titled “CONS OID TMP” and “CONS OID PRM” can be located within Police Forms, within the “HTCG” section.

Personal personas

No personal personas (disused, obsolete, or otherwise) associated with past or current Police employees or associates will be utilised for any roles outlined in this chapter unless by consent or required by unique operational circumstances.

Open-Source Information and Online Practitioner

It is recognised that most intelligence gathering activities and investigations into criminal offences now have an online component to them. Evidence or information posted on Social Networking sites or other forums can create or direct phases of investigation and assist with developing target profiles, associates, and attribution.

Police have adopted a framework which defines how information and evidence is identified from online sources and by whom. These five roles each outline specific expectations and restrictions:

- Overt Online
- Discreet Online Passive Operations
- Discreet Online Active Operations
- Discreet Online Controlled Operations
- Discreet Online Advanced Operations

Role 1: Overt Online

This role describes the knowledge and skills required to conduct general queries overtly online. The purpose of this role is to facilitate police activities on the internet.

This role describes the online capabilities required for individuals whose duties require performing activities and engaging online as a police employee, e.g., public affairs, community policing teams, or prevention initiatives.

An employee performing this role **does not** utilise an online persona (assumed identity).

For further instruction on using social media for community engagement and guidance on private use, see ‘Social media policy’.

Role 2: Discreet Online Passive Operations

This role describes the knowledge and skills required to conduct discreet research using the internet.

This is the most common role within Police.

A risk assessment for discreet research will be completed and authorised by a supervisor of at least the rank of Sergeant.

Practitioners will have successfully completed training to **Level 1** of the National Cybercrime Training Programme and will be fully conversant with legislative and policy guidelines and restrictions.

- An employee performing this role may utilise an overt identity if risk of discovery has been assessed as minimal and/or insignificant.
- An employee performing this role may utilise a registered assumed identity if risk of discovery has been assessed as possible and/or likely.
- An employee performing this role remains passive s.6(c) OIA.
- Where utilising an online persona an employee performing this role may be utilising s.6(c) OIA as outlined in the ‘Equipment’ section of this chapter.
- A Discreet Online Researcher s.6(c) OIA

Note: Currently the Level 1 training consists of 4 e-learning modules available in Success Factors.

Role 3: Discreet Online Active Operations

This role describes the knowledge and skills required to apply online capabilities to investigate crimes and gather intelligence using registered personas.

A risk assessment for deployment of the registered persona will be completed and authorised by a supervisor of at least the rank of Senior Sergeant.

Practitioners will have successfully completed the online elements of **Level 1** of the National Cybercrime Training Programme and will be fully conversant with legislative and policy guidelines and restrictions including the Police instructions mentioned above.

- At the Senior Sergeant's discretion, an employee performing this role may utilise a registered assumed identity.
- An employee performing this role will have s.6(c) OIA
- A Discreet Online Persona maintains s.6(c) OIA
- An employee performing this role may be utilising s.6(c) OIA as outlined in the 'Equipment' section of this chapter.

Role 4: Discreet Online Controlled Operations

This role describes the knowledge and skills required to support and contribute to workgroups in specialised areas, s.6(c) OIA

A risk assessment for deployment of the registered persona will be completed and authorised by the relevant Manager or equivalent.

Practitioners will have successfully completed the online elements of **Level 1** of the National Cybercrime Training Programme and specific Covert Online Training and will be fully conversant with legislative and policy guidelines and restrictions.

- An employee performing this role will utilise a registered assumed identity.
- An employee performing this role will have s.6(c) OIA
- An employee performing this role will be utilising s.6(c) OIA as outlined in the 'Equipment' section of this chapter.
- The role of Discreet Online Controlled Operations s.6(c) OIA

Role 5: Discreet Online Advanced Operations

This role describes the knowledge and skills required by individuals who are targeting offenders with s.6(c) OIA. The Discreet Online Specialist will possess high level skills and knowledge of the investigation intricacies to ensure credibility is maintained [redacted] s.6(c) OIA

A risk assessment for deployment of the registered persona will be completed and authorised by at least the Manager High Tech Crime Group, NOCG, or National Security.

Practitioners will have successfully completed the online elements of **Level 1** of the National Cybercrime Training Programme and specific Covert Online Training as well as additional specialist training provided by the Cybercrime Unit. Practitioners will be fully conversant with legislative and policy guidelines and restrictions.

- An employee performing this role will utilise a registered assumed identity.
- An employee performing this role will have s.6(c) OIA
- An employee performing this role will be utilising s.6(c) OIA as outlined in the 'Equipment' section of this chapter.
- A Discreet Online Specialist s.6(c) OIA

Equipment

Careful consideration needs to be taken to ensure that the right equipment is being utilised when operating an online persona.

s.6(c) OIA

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

All non-attributable systems must be implemented in accordance with guidance from the High Tech Crime Group or the s.6(c) OIA

Accounts on social media and other services

Anyone operating at levels 2-5 is likely to need to create accounts across a range of services to enable access to required information. Care should be taken to minimise the risk of attribution of staff activity to the Police. Staff in roles 2-5 should:

- not use personal devices, email addresses, or phone numbers to register for services.

s.6(c) OIA

- make themselves familiar with the security settings on their account and ensure accounts are secured from public viewing as much as is practical

s.6(c) OIA

Cellular/mobile phone verification

When registering your online persona with various applications, you may be required to supply a cellular/mobile phone number to verify or activate the account. You should assess the objectives of the online persona created and evaluate if you wish to supply a non-attributable cellular/mobile number to the service.

In exceptional circumstances you may wish to consider the cash purchase and activation of a pay-as-you-go cellular/mobile phone.

Home or personal device

A personal computer system or device must **not** be utilised for any roles outline in this chapter.

Evidence capture

Methodology

It is essential that online information or investigation activity can be recorded, to prove how the information or evidence was obtained. Methods of documenting online investigative processes can include, but is not limited to:

- comprehensive notebook entries
- screen prints
- photographing or videoing the screen interactions
- third-party software designed to capture data.

At a minimum, any capture should record the individual’s QID, date, time, URL, and file name of the capture. Snipping part of a page without recording the other data limits the future use of the capture in an evidential capacity, even if the initial capture is for intelligence purposes.

Advice should be sought from the Cybercrime Unit regarding evidence capture methods.

Social Networking chapter

It may be possible to recover information or evidence of your interaction retrospectively. Refer to the‘Social Networking Guide’ for further information. Note, that the Guide is always being updated as new providers are identified or responses to requests change.

Disclosure

For prosecutions, Police must comply with the Criminal Disclosure Act 2008. It is essential that a detailed record of any online activities is fully documented so that obligations under the Act can be met.

Organisational risk

Although some risk-taking is inevitable in the execution and pursuit of our objectives, being risk aware means that we not only actively manage potential problems, but also identify potential opportunities. To manage risk, we need to identify and evaluate the risks we face as an organisation and identify the controls needed to mitigate these risks.

Reducing organisational risk

Organisational risk is reduced when Police employees follow the key operating principles in this chapter.

Disclosure of online investigations methodology

Every effort should be implemented to safeguard the disclosure of Police methodology and techniques when conducting online investigations. [redacted] s.6(c) OIA

The disclosure of a Police persona and its use in a covert operation is likely to cause significant media attention and may impact on the organisation's reputation.

[redacted] s.6(c) OIA

[redacted]

[redacted]

Legislation

As Police utilise the internet as a source of information and evidence it needs to comply with New Zealand Legislation. The New Zealand Bill of Rights Act 1990, the Privacy Act 2020, the Crimes Act 1961 and the Search and Surveillance Act 2012 all have sections that limit what Police can lawfully do.

There is a fine line between what is in the public domain and what is not, and therefore Police need to mitigate any organisational risk by evaluating legislative implications and ethical obligations.

Police may be required to justify that their actions were lawful, ethical, reasonable, consistent, and proportionate to operational requirements.

Some activities may require a search warrant. Early liaison with Police Legal Services is recommended where there are concerns that the information may not be considered to be in the public domain.

Committing offences

Current legislation does not permit Police to commit any offence for the purpose of progressing with an investigation other than outlined in the Misuse of Drugs Act 1975, relating to the protection of undercover officers.