



He Kaupare. He Manaaki. He Whakaora.
Prevention. Care. Recovery.

Information Gathering Guidelines

Fraud Prevention and Investigation

August 2025

For: Fraud Prevention and Investigation Team

Document Owner: Integrity Outcomes and Resolution Manager

Publish Date: October 2024

Reviewed (Unit name change) August 2025

Review Date: October 2026



Contents

Purpose.....	3
Principles.....	4
Definition: Covert Information Gathering.....	5
Definition: Overt Information Gathering	6
What we don't do.....	7
Mental Health Issues.....	7
Covert Information Gathering	
Surveillance.....	9
Court Orders.....	9
Requests for Information (RFI).....	11
Internal Requests for Information (IRFI).....	11
Covert Internet and Social Media searches.....	12
Overt Information Gathering	
Overt Internet and Social Media searches.....	14
Reporting.....	15
Training.....	16
Complaints.....	16
Information Illegally Obtained.....	16
Relevant Legislation.....	17



He Kaupare. He Manaaki. He Whakaora.
Prevention. Care. Recovery.

Purpose

These guidelines outline the protocols for Fraud Prevention and Investigation staff and its contractors that must be followed to gather information during an external Fraud investigation or intervention. The guidelines can also be used as guiding principles for all other ACC staff regarding information gathering related to Integrity related issues.

The guidelines should be read in conjunction with the ACC corporate policies “Social Media Policy” and “ACC Integrity Information Gathering Policy” and supersede any previous versions, standard operating procedures or other documents that contain similar content.

This document does not and should not limit or impact the collection of information for non-fraud investigation related purposes, or pursuant to any other agreement such as an Approved Information Sharing agreement (AISA), Memorandums of Understanding (MOU), information obtained or collected in accordance with relevant Privacy Principles, pursuant to the Privacy Act 2020, any other legislative authority or information collected for other purposes such as determining entitlements or understanding health or medical related matters in accordance with the Accident Compensation Act 2001.

Public servants must be vigilant in how they exercise the significant responsibilities and powers entrusted to them by New Zealanders. This is fundamental to the integrity of the public service. ACC must ensure that the way we use our authority to collect information is not only lawful but supports public trust.

There may be occasion for other ACC business units to utilise information gathering activities (e.g. online data mining) and any such activity should ensure that it complies with relevant corporate policies irrespective of role, mandate, or function.

ACC Fraud Prevention and Investigation staff and contractors are expected maintain the highest standards of integrity, discretion, and ethical conduct and to follow the ACC Code of Conduct. Any action that is in breach of the ACC “Social Media Policy” and “ACC Integrity Information Gathering Policy” or the Integrity Information Gathering guidelines or other associated guidelines may result in a Code of Conduct investigation and disciplinary action.

If in doubt regarding these information gathering policies or guidelines, please contact ACC Fraud Prevention and Investigation at email Integrity.services@acc.co.nz



Principles

Before undertaking any information gathering, the following guiding principles must be considered:

These principles guide us when we are building an understanding of behavioural context:

1. Start at Source – obtain consent from client / provider / vendor if possible.
 - Exceptions to starting at the source need to be clearly justified - Other options have been considered and are inappropriate in the circumstances.
 - Exceptions to starting at the source must be supported by clear evidence-based rationale.
2. Proportionate, balanced, appropriate, and lawful
 - **Proportionate:** Is the level of intrusion into the privacy of an individual or organisation justifiable in the circumstances of the allegations made
 - **Balanced:** Any such activity cannot be conducted without careful consideration and in recognition of all relevant circumstances.
 - **Appropriate:** Any such activity must be ethical, appropriate and be aligned to legislative requirements and the code of conduct for ACC and the Public Services Commission.
 - **Lawful:** Any activity must comply with relevant legislation¹ including the 13 Information Privacy Principles in the Privacy Act 2020 and the policy statements contained within ACC's Personal Information and Privacy Policy².
3. Information Gathering using high standards of discretion and ethical conduct.
4. Any Risks, real and perceived, must be escalated to your manager.
5. All relevant privacy, policy and principles apply.
6. Health and Safety policy and principles apply.

Our interventions are guided by Enquiry Guidelines:

- Proactively engaging with our customers – internal and external
- Interventions should follow the enquiry process – assess, explore, inquire, resolve, close the loop.
- Influencing people to “do the right thing” (Whaia Te Tika)
- Ensuring we close the loop to continually monitor, adapt and communicate throughout each step of the process.

¹ Privacy Act 2020; New Zealand Bill of Rights Act 1990, Search and Surveillance Act, 2012, Crimes Act 1961 and any relevant Court decisions.

² Personal Information and Privacy Policy, 18 June 2024



Definition: Covert Information Gathering

Covert information gathering is anything collected without the subject's knowledge or consent in circumstances in which the subject would reasonably expect the information to be private.

Covert information gathering activities can only be authorised or utilised by ACC Fraud Prevention and Investigation staff or after gaining approval from a Fraud Prevention and Investigation Manager.

Covert information gathering should not be undertaken unless all efforts to obtain consent to obtain the information from the source or with the consent of the client, provider or vendor have been exhausted, or where one or more of the following exceptions apply:

- Where circumstances exist to satisfy Part 3 of the Search and Surveillance Act 2012 relating to surveillance device warrants and production orders
- Where circumstances exist to satisfy Part 4 of the Search and Surveillance Act 2012 relating to search warrants
- Where there is significant risk to life or property and the use of covert information gathering will mitigate such risk
- Where the risk of loss to the ACC and/or the nature of the suspected offending against the ACC justifies the use of covert information gathering and Privacy Principle 11 permits the sharing of information between agencies in limited circumstances.
- Where advising or requesting information from the client, provider or levy payer first may lead to interference with evidence or witnesses or lead to further criminal offences being committed.

Types of covert information gathering include, but are not limited to:

- Visual surveillance, including with the use of a visual surveillance device and by observation with the naked eye.

Examples include:

- Video cameras (whether recording or live streaming)
- Still cameras (with or without zoom and other types of lenses attached)
- Binoculars and night vision equipment
- Drive past a client's address with the deliberate purpose of observation.
- Observations in a public place (e.g. sports field, shopping mall etc.)
- Following clients (e.g. vehicular or on foot)



- Obtaining private information by way of production order or search warrant in accordance with the Search and Surveillance Act 2012 without the knowledge or consent of the subject.

Examples Include:

- Telecommunications Records
- Banking Records
- Employment Records
- Clinical Records
- Computer Activity Reports

- Requests for Information (RFI) from other agencies or private enterprises or internally without the knowledge or consent of the subject.

Examples include:

- Travel history checks.
- Passport photos
- Banking records
- Contact details.
- Income details

- Open-source online information gathering using a pseudonym.

Examples include:

- Use of social media (Facebook, LinkedIn, Twitter, Instagram etc.) under an account created with false information.

Definition: Overt Information Gathering

Overt information gathering is data collection used in open or in plain sight.

Overt information gathering is likely to consist of utilising open source or publicly available online sources to gather information regarding a client, provider, or levy payer.

Types of Overt information gathering could include:

- Search engines (e.g. Google and Bing).
- Aggregated Information Services (e.g. Infolog)
- Use of social media under an organisational account

Overt information gathering should not be conducted in the normal course of business unless:

- The client has provided consent, or
- The information is obtained or provided to ACC unsolicited (i.e. because of search algorithms) or



- The information gathering relates to a client safety issue or
- The information gathering is part of a recognised investigation being undertaken by a member of the Fraud Prevention and Investigation team and there is specific reference to social media content (see SM Policy/Information gathering policy).

Information gathering, what we don't do.

Over the passage of time, information gathering techniques and technology changes. Innovative ways to collect information may be identified but must not be utilised unless prior ACC Fraud Prevention and Investigation management (via your line manager) approval is sought and granted in writing.

Inappropriate activities include, but are not limited to:

- Utilisation of tracking devices (including GPS devices) to track clients, providers or other persons of interest or vehicles.
- Utilisation of listening devices or intercepted electronic conversations.
- Use of drones or other aerial devices for observation purposes.
- Conducting pretext calls using fictitious or assumed identities.

Appropriate consideration must be given to any impact that information gathering may have on the management of the claim, and any associated risks. This may include effects on the wellbeing of:

- the client, because of their individual circumstances
- the case owner
- the staff member or contractor.

It is **not** acceptable to:

- Classify a person or group of people as a security threat - and use that as justification for gathering information, solely because they lawfully exercise their democratic rights.
- Gather information about people or groups for the sole purpose of managing reputational risk to ACC.

Mental Health issues

Except in exceptional cases, where the person of interest has documented serious mental health issues of a nature that may cause serious danger to that person's health and safety or the health and safety of any other person, **visual surveillance should NOT be conducted.**



Any covert Information Gathering must be reasonable in all the circumstances (including the mental health status of the subject), to comply with s21 of the New Zealand Bill of Rights Act 1990 (which protects people from unreasonable search and seizure).

If an exceptional case is identified, it is to be considered by the Fraud Prevention and Investigation manager in conjunction with the appropriate subject matter experts and formal approval must be gained and documented before proceeding.

Distress/ fear

Where a client's circumstances may lead to information gathering and/or surveillance causing the subject to experience distress or fear, the following steps should be taken:

- Consult the appropriate ACC case manager to discuss the potential effect of the activity.
- The Integrity Advisor or Investigator should be satisfied that it is appropriate to continue with information gathering and must consult their supervisor / manager before progressing.
- If the Manager agrees to progress and surveillance is required from an external contractor, they should be informed of any relevant issues and ensure that extra precautions are taken to reduce the prospect of fear or distress occurring.



Covert Information Gathering

Surveillance

All covert surveillance activities must be conducted in accordance with relevant legislative requirements (specifically the Search and Surveillance Act 2012) and must comply with relevant ACC policies and guidelines.

The use of covert surveillance activity should only be considered after all other appropriate and relevant lines of enquiry or investigative techniques have been exhausted or determined to be impractical.

Surveillance of individuals in private spaces should only be considered in exceptional circumstances and where a Court issued surveillance device warrant has been issued. Such surveillance will not be conducted unless authorised by the Court.

Authorisation for any proposed covert surveillance must be obtained from the Fraud Prevention and Investigation Manager after consultation with Legal and Privacy advisors.

Surveillance will only be carried out by accredited, qualified, and experienced people. Generally, this will be a specialist operative selected from our approved list of suppliers and engaged pursuant to the “*ACC Investigation Support Panel*”.

In exceptional circumstances, an ACC Integrity Advisor, trained in surveillance, may be approved to conduct visual surveillance.

Prior to conducting any surveillance, any risks posed by the client, provider or levy payer must also be identified (as per the [Worksafe Policy](#)), and discussed with the Fraud Prevention and Investigation Manager. Any risks must be disclosed to the supplier/contractor to ensure they follow their own health and safety protocols.

For specific guidance on surveillance activities see the Fraud Prevention and Investigation quick guide for surveillance operations.

Obtaining private information by Court Order

Obtaining private information by way of Court order may include production order applications or search warrant applications without the knowledge or consent of the subject to obtain private information held regarding a subject.



Search warrants & production orders can only be applied for and executed by the NZ Police (or an authorised person) and are subject to the provisions contained in the Search and Surveillance Act 2012.

The use of production orders or search warrants to obtain private information relating to a subject should only be considered if the client has previously been lawfully requested to provide the information and has refused, or has failed to engage with ACC investigators unless the following exceptions apply:

- Where notifying or seeking information from the client may lead to interference with witnesses or evidence or
- Where evidential material may be lost or destroyed due to time constraints if consent is obtained first.

All applications for search warrants must meet the evidential threshold; that there are reasonable grounds to suspect that a criminal offence has occurred (or is occurring or will occur), and that there are reasonable grounds to believe that the search will find evidential material in respect of the criminal offence.³

All applications for production orders must meet the evidential threshold; that there are reasonable grounds to suspect that a criminal offence has been committed (or is occurring or will occur), and that there are reasonable grounds to believe that the documents sought constitute evidential material in respect of the criminal offence, and that those documents are in the possession or under the control of the person against whom the order is sought.⁴

All applications for production orders or search warrants must be reviewed by and approved for submission by ACC legal counsel prior to submission.

Examples of information sought by way of court order may include:

- Telecommunications Records
- Banking Records
- Employment Records

Any information gained by ACC because of a Court order must only be used, stored or shared in accordance with the conditions set out in the Court order issued.

Any private information gained by ACC investigators by way of Court order must be kept securely, not distributed outside of those required to use the information during the

³ Search and Surveillance Act 2012, s 6.

⁴ Search and Surveillance Act 2012, s 72.



investigation to which it relates and not made available to any other workgroups or agencies without review by Privacy and Legal advisors.

Request for Information (RFI)

Interagency RFI's are governed by the Privacy Act 2020, Accident Compensation Act 2001 and other information gathering protocols (e.g. Section 72, 241, 279 or 309, AC Act 2001) and must comply with the appropriate principles contained within the relevant Acts.

All RFI's must comply with the relevant legislation under which the information is sought.

Prior to submitting an RFI, the person whom the request relates should either be asked to provide the information themselves or asked to give informed consent for ACC to request the information.

Consideration can be given to requesting information without the consent of the person involved in the following circumstances:

- If the person refuses to or fails to provide the information and there are legitimate and justifiable reasons to continue to seek the information or.
- If the person refuses to provide consent for the information to be requested and there are legitimate and justifiable reasons to continue to seek the information or.
- If the information requested is required to advance a criminal investigation and requesting consent or advising the subject of the request would likely result in interference with witnesses or evidence or.
- If the circumstances of the investigation require obtaining information to locate or confirm contact details for a client and that information is not available from ACC sources or the client is not contactable or unavailable.

If any of the circumstances outlined above apply, this should be discussed with a supervisor/manager and decisions documented to ensure there is appropriate justification to proceed.

In submitting an RFI, it should be recognised that the agency that holds the information decides if it is appropriate to release that information.

Informal information gathering, such as the use of interagency contacts to gather information pertaining to a private citizen (e.g. travel movement history), is not to be undertaken outside of recognised RFI procedures as it may compromise the subject's right to privacy and be perceived as unfair or unlawful.



Where there is an immediate risk of harm, health and safety concerns are identified, or criminal history or intelligence is sought, then these request types must be channelled via the ACC Safety Partners team for advice and support.

Internal Requests for Information (IRFI)

In some circumstances client, provider or levy information is collected by the ACC directly from the source or from other agencies for specific purposes. This information may be of assistance to advance an investigation but would not normally be available to use for such purposes.

- An example is RTE information collected for the purpose of setting up weekly compensation or levy information collected for the purpose of calculating ACC levies.

This information is not usually available to investigators as it would be used not for the purpose for which it was collected.

Should this information be required for the detection, investigation, prosecution, and punishment of offences, investigators may consider requesting the information via an internal request for information.

All factors relating to external RFI's (see section above) apply to IRIF's.

See "IS guide for investigators on use of IRIF's" for further information⁵.

Covert Internet and Social Media searches

Searches conducted using subterfuge, fictitious identities or pseudonyms must not be undertaken without express approval of the Fraud Prevention and Investigation Manager.

If Fraud Prevention and Investigation receive an allegation of organised or serious crime or information is identified that indicates an actual or potential risk of harm to a person or persons (including ACC staff), then covert internet or social media searches, using a pseudonym account may be considered.

Considerations can include:

- The allegation contains direct reference to organised crime.

⁵ Please note – this IRIF process is not currently active, and some further consultation is required. It has been included at this time to future proof the guidelines. The prescriptive guide for use of IRIF's will be completed after consultation with relevant parties.



- The allegation source is credible (e.g. from another Government agency either domestic or offshore).
- The allegation contains reference to an imminent risk or threat of serious personal harm.
- There are concerns around the disposal, destruction or alteration of evidence that may lead to the detection of a serious offence.
- There is an active care indicator associated to the person about whom the allegation is being made.
- The subject of the allegation is being managed by the Remote Claims Unit.
- The subject of the allegation has known links to Outlaw Motorcycle Gangs (OMCG's) or other organised criminal groups.
- The allegation contains specific threats to a person or persons.

The use of covert internet or social media searches is an exception and should not be used outside the considerations outlined above and must only occur after consultation with a manager. Any decisions made and the rationale for those decisions should be carefully documented.



Overt Information Gathering

Internet searches & Social Media

Open-source or publicly available social media information gathering is considered overt in nature.

ACC staff must not use any publicly available online source, including any social media platforms, to collect information about clients without their knowledge or consent (see social media policy⁶).

The only exception to this policy is for Fraud Prevention and Investigation and Workplace Integrity Team staff.

Overt internet or social media searches should only be undertaken by Fraud Prevention and Investigation staff if there has been information provided that indicates that online content is available that relates specifically to the matter under investigation.

The following matters should be considered prior to seeking the clients consent and undertaking any online activity.

- The information must be publicly available
- Any such open-source search must be lawful and reasonable.
- The open-source search must be justifiable in terms of the specific investigation being conducted
 - For example: The referral or allegations directly references social media content that corroborates the allegation.
- Any search for information is necessary to prevent, detect, prosecute, or punish offences.
- The subject of the allegation (unless maintenance of the law exceptions apply) should be advised of the allegation and be asked to provide the information themselves or give consent for ACC to review or collect the content.

Should the investigator believe that seeking the client's consent is likely to facilitate the destruction of evidence, or interference with witnesses, or if the client is unable or unwilling to provide consent, consideration can be given to completing online searches without the client's consent.

Prior to conducting any unconsented online searches, the following steps should be taken:

⁶ Note: This paragraph is not currently in the Social Media policy but is an addition that has been proposed by FPI for inclusion in the next policy review.



- Discussion with a Fraud Prevention and Investigation supervisor/manager to confirm that any decision is in accordance with ACC policies and guidelines.
- Document all considerations and decisions.
- Give full consideration is given to whether the information sought is crucial to the advancement of the investigation and/or whether the search is likely to produce relevant evidence.

Conducting social media or internet searches without a valid reason to gain general information, or as a “fishing expedition” is not justified.

Contractors must ensure they abide by these rules. If in any doubt, please seek advice from the Fraud Prevention and Investigation Manager.

For further guidance on social media see “Fraud Prevention and Investigation Guidelines for the use of Social Media” (dated 16 June 2022)

Guidance for non- Fraud Prevention and Investigation staff regarding social media

Should information relating to a Fraud or integrity issue involving a client, provider or vendor be inadvertently obtained via social media, (for example social media algorithms promote content relating to a specific client) this information should be noted and referred to Fraud Prevention and Investigation and no further searching or enquiries should be completed by ACC staff unless they are a member of the Fraud Prevention and Investigation Team.

Where a Fraud or integrity concern is raised regarding a client, provider or vendor that suggests that further information is available either online or via some other method of enquiry, any information gathering undertaken as part of that concern or referral should only be completed by a member of the Fraud Prevention and Investigation team.

Reporting

A regular reporting regime is required as part of the activation and ongoing monitoring of any Covert Information Gathering activity. This includes:

- Front end: Decision making framework, approvals process, rationale, H & S risk briefings and recording.
- In-flight: Regular updates and incident reporting (including “near misses”)
- Retrospective: ACC Fraud Prevention and Investigation internal and external reporting.



He Kaupare. He Manaaki. He Whakaora.
Prevention. Care. Recovery.

Training

Any person to which this guideline applies (whether internal or external) must attend regular refresher training. This will include how to be compliant with the decision-making process that is required when undertaking information gathering, especially covert types. It will also emphasise the importance of public perception and our responsibilities associated with undertaking information gathering.

Complaints

In the event of a complaint being made either directly with an ACC Integrity Advisor, contractor, or other ACC staff member (e.g. case owner or call centre staff member) then this shall be deemed as an activation of the formal complaint process. Complaints can also be channelled through the client resolution team. The ACC Fraud Prevention and Investigation Manager must be advised of any formal complaints.

Information Illegally Obtained

Personal information is taonga (treasured), and we consider ourselves to uphold the principles of Kaitiakitanga (stewardship) of any personal information we receive.

For the purposes of these guidelines, personal information includes health information.

We are committed to managing personal information in line with the Privacy Act 2020, the Health Information Privacy Code 2020, any related legislation and recognised best practice.

As per the Personal Information and Privacy Policy the ACC has a wide range of statutory functions and duties under the Accident Compensation Act 2001.

We collect, use, store and share personal information to fulfil those functions and duties, as well as for related lawful activities. We are entrusted with personal information. It is fundamental that we protect this information and use it only for permitted purposes and in appropriate ways.

Any unsolicited information received by the ACC, or information collected by ACC staff or contractors in a manner that suggests that it has been collected, obtained or shared in breach of any relevant legislation (for example; collecting information on a person that would be considered harassment pursuant to the Harassment Act 1997, accessing a computer system or conducting surveillance in a private place without appropriate orders pursuant to the Search and Surveillance Act 2012), will be reported to the appropriate authorities.



He Kaupare. He Manaaki. He Whakaora.
Prevention. Care. Recovery.

This may include:

- Filing a criminal complaint with the NZ Police
- Filing a notifiable privacy breach with the Privacy Commissioner
- Advising any other appropriate statutory body.

Such activity if undertaken by ACC staff members may also result in a Code of Conduct investigation.

Relevant legislation

The following legislation and codes are relevant to visual surveillance⁷:

- Accident Compensation Act 2001
- ACC Code of Conduct
- Code of Claimants rights
- Code of Conduct for the State Services
- Crimes Act 1961 No 43 (as at 18 April 2012)
- Evidence Act 2006 No 69 Section 30⁸
- Harassment Act 1997
- Health Information Privacy Code 2020
- New Zealand Bill of Rights Act 1990 No 109 (as at 01 February 1994), Public Act – New Zealand Legislation
- Privacy Act 2020⁹
- Private Security Personnel and Private Investigators Act 2010
- Private Security Personnel and Private Investigators (Code of Conduct—Surveillance of Individuals) Regulations 2011
- Search and Surveillance Act 2012
- Summary Offences Act 1981, Sections 29 & 30
- Trespass Act 1980 No 65

⁷ Courts have treated some forms of surveillance conducted by law enforcement agencies as “searches” for the purposes of s 21, and it should therefore be assumed that any visual surveillance is required to be “reasonable” under this section).

⁸ Relevant to the admissibility of evidence in court that has been gained as a result of unlawfulness or an unreasonable search)

⁹ Relevant to dealing with the information gained as a result of visual surveillance