



Privacy Policy

October 2021

Purpose

The Invercargill City Council is committed to ensuring that it follows best practice whenever it handles personal information and in doing so maintains the privacy rights of individuals.

Whilst this Policy sets out the responsibilities and procedures for the collection, use, retention and disclosure of personal information and has been prepared in accordance with all of the obligations and rights set out in the Privacy Act 2020. However ICC's overarching principle is that personal information will only ever be collected for a lawful purpose connected with a Council function or activity and only when that collection is necessary for that purpose.

This document is intended to be a resource for employees and a source of information for members of the public.

Scope

This Policy applies to all employees, elected members and committee members of the Invercargill City Council, including volunteers or people engaged or contracted under a contract for services (contractors) for the Council. The term "employee" will be deemed to mean all persons that are covered by this policy.

Definitions

Personal information

Means any information which discloses something about a specific individual. The information does not need to name the individual, as long as they are identifiable in other ways, like through their home address or employee number.

As a result all sorts of things can contain personal information, including notes, emails, recordings, photos and scans, whether they are in hard copy or electronic form.

Roles and Responsibilities

Privacy Officer

The delegated Privacy Officers for the Invercargill City Council are Strategic Advisor/General Manager ICHL and Manager – Quality Assurance whose responsibilities include:

- The encouragement of compliance, by the Invercargill City Council, with the information privacy principles.
- Dealing with requests made to the Invercargill City Council pursuant to the Privacy Act 2020.

- Working with the Commissioner in relation to investigations conducted pursuant to Part 5 of the Privacy Act in relation to the Invercargill City Council.
- Otherwise ensuring compliance by the Invercargill City Council with the provisions of the Privacy Act 2020.

The Chief Executive has the principal obligation to ensure this Policy and the Privacy Act 2020 are being complied with.

The Privacy Officers shall ensure compliance with this document. As required, but at least annually, the Privacy Officers shall report to the Chief Executive in accordance with the Governance Document Framework and Governance Framework.

Principles

Section 22 of the Privacy Act 2020 sets out 13 privacy principles that specify how information can be collected and used, and people's rights to gain access to that information and ask for it to be corrected.

Invercargill City Council understands that people need to be able to protect information about themselves and will balance this right with the requirement to collect and hold certain information in order to carry out its functions.

These principles do not apply to public registers including the rating database (Section 11 Local Government (Rating) Act 2002) nor does it apply to the electoral roll required for Local Elections (as requires by the Local Electoral Act 2001 - noting the ability for people to be on the unpublished roll).

Appendix A lists the 13 privacy principles and how Council applies them.

Invercargill City Council Customer Privacy Policy

What kind of personal information does Invercargill City Council collect?

The personal information we collect may include name, date of birth, addresses, email address, telephone numbers, gender, information on the use of our services or facilities and any other information provided by an individual in connection with, or specifically related to their communications with us or, their use of our services or facilities.

Collecting your information

We may collect personal information about an individual as set out below:

- Personal information may be collected when an individual or someone authorised by an individual to act on their behalf provides information to us directly. For example when they:
 - Apply for employment with us.
 - Correspond with us, whether in person, by letter, phone, text, email, instant messages or other means of electronic communication.
 - Complete and submit forms we provide for applications for consents, licences, approvals, permits, funding or other authorisations or for the use of any of our services or facilities, including signing up for and using our online services and apps.
 - Prepare and submit a written submission, request or other feedback in relation to applications for consents, licences, approvals, permits, funding or

other authorisations, or in relation to any form of draft or proposed plan, policy, bylaw or other document.

- Use any of our services or facilities.
- Subscribe to any of our newsletter or update services.
- Follow or post comments in response to our social media or other facilities, including but not limited to, Facebook, Twitter, Instagram and YouTube.
- We may keep a record of any information that they acquire from us.
- We may monitor and record phone calls made to or by us for quality control or staff training purposes. If a call is to be monitored and/or recorded, the participants will be informed of this at the time of the call.
- We may collect personal information from other organisations, entities or persons, such as:
 - Our related organisations including Council Controlled Organisations.
 - Our suppliers which include organisations such as:
 - Land Information New Zealand
 - QV
 - Solicitors/conveyancers.
 - The New Zealand Police, credit reporting agencies and other organisations, entities and persons where individuals have expressly authorised them to provide us with information.
- When anyone visits one of our websites, we may utilise technology solutions such as browser cookies to collect non-identifying information about how our websites are being used. This information is only analysed on a bulk basis for aggregate website traffic usage and geolocation purposes. Additionally, internet service providers and our internet service provider may record visits and log the information for statistical purposes. We do not attempt to identify individual users or analyse their browsing activities unless they choose to give us personal information while using our website.
- “Closed Circuit Television” (CCTV) is used in particular areas to monitor public transport passenger safety and security, public transport park and ride facilities, and for environmental monitoring purposes.
- When appropriate, signage advising of CCTV equipment will give notice of areas covered by such equipment. CCTV footage will only be viewed by authorised people in accordance with the purpose noted above or for the purposes of regularly checking the system is operational. No attempt is made to identify individuals from CCTV footage except in relation to a reported or suspected incident requiring investigation.
- “Wearable cameras” are used by enforcement officers to record interactions. When used the officer will inform the individual that the wearable camera is in use. The footage will only be viewed by authorised people in accordance with this purpose and in relation to a reported or suspected incident requiring investigation. Refer to Invercargill City Council Wearable Video Camera Guidelines.

Using the information we collect

The personal information that we collect may be used for any of the following purposes:

- To provide individuals with services or facilities, including:
 - those that have been requested; and

- assisting our Council Controlled Organisations to provide such services or facilities to individuals.
- To positively confirm an individual's identity. This is to avoid inappropriate release or use of information.
- To respond to correspondence or to provide individuals with information that they have requested.
- To process applications for any consent, licence, approval, permit or other authorisation for which individuals have applied.
- To process applications to use or to register for any of our services or facilities, including our online services.
- To respond to requests, enquiries or feedback, or for customer care related activities.
- To provide individuals with information about our events, news, services or facilities, or the events, news, services or facilities of our Council Controlled Organisations that we consider may be of interest. Individuals will have the option of unsubscribing from these communications.
- To comply with relevant laws and regulations including by commencing proceedings in Court.
- To carry out activities connected with the running of our operations such as personnel training, or testing and maintenance of computer and other systems.
- For any specific purpose which will be disclosed at the time the personal information is collected.
- For general administrative and business purposes.

Sharing your information

We may disclose personal information about individuals to:

- Any person engaged by the council to provide products or services on our behalf, where personal information is necessary for the provision of those products or services.
- Council Controlled Organisations, in order to assist with the functions and services that they provide.
- A third party if we are required to do so under any laws or regulations, or in the course of legal proceedings or other investigations. This may include sharing CCTV footage with the New Zealand Police or other public sector agencies where criminal activity is reported or suspected. The New Zealand Police may also access live feeds from certain CCTV cameras from time to time, for law enforcement, investigation and emergency response purposes.
- Any person who an individual authorises us to disclose their personal information to.
- Any person, if that information is held in a public register, e.g. information held on the rating information database.

What happens if an individual does not provide us with the personal information requested?

If an individual does not provide us with all of the personal information that we have requested, we may not be able to adequately respond to their correspondence, process any applications they have submitted, provide the services or facilities they have requested, process payments or otherwise deal with any requests or enquiries they have submitted.

In some circumstances, failure to provide information when requested may be unlawful, and/or result in legal consequences. These circumstances and the potential consequences will be explained to individuals when their personal information is collected.

Security and accuracy

We take reasonable steps to ensure personal information is:

- protected against loss, damage, misuse and unauthorised access. We restrict access to personal information to those individuals who need access to this information in order to assist us in performing our duties and obligations
- accurate, up to date, complete, relevant, and not misleading.

How long we hold personal information?

We will retain all of the personal information we collect (on both our active systems and our archive systems), for as long as administratively necessary, in accordance with the council's information retention and disposal schedule.

The Public Records Act 2005 requires us to retain "protected records" indefinitely. In some circumstances, personal information may be included within a protected record, including submissions that individuals make in relation to bylaws, annual plans, and regional planning instruments.

Accessing and correcting your personal information

Individuals may request confirmation of whether or not we hold any personal information about them and they may request access to your personal information that we hold by emailing us at service@icc.govt.nz or otherwise contacting us, at the addresses provided below. Once we have verified their identity we will provide them with such confirmation and access unless one of the grounds for refusal to do so under the Privacy Act 2020 applies.

Individuals may request that the personal information we hold about them be corrected by emailing us at service@icc.govt.nz. If we agree that their personal information is to be corrected we will provide them with an amended record of their personal information if requested.

Any rights of access to and correction of any personal information we hold are subject to the procedures set out in the Privacy Act 2020.

Compulsory notification of breach

Section 114 of the Privacy Act 2020 requires that the Commissioner must be notified of a notifiable privacy breach. A notifiable privacy breach is a privacy breach where it is reasonable to believe it has or is likely to cause serious harm. A privacy breach is defined as unauthorised access to, disclosure, alteration or loss of personal information.

When assessing whether a privacy breach is likely to cause serious harm the following must be considered:

- any action taken to reduce the risk of harm;
- the sensitivity of the information;
- the nature of the harm;
- any recipient of the information as a result of the breach;
- whether the information is protected by a security measure; and
- any other relevant matters.

Who can be contacted for further information

For any queries regarding this Privacy Policy or personal data Invercargill City Council has collected, please contact Invercargill City Council's Privacy Officer.

Email address: service@icc.govt.nz
Postal address: Invercargill City Council
101 Esk Street Private Bag 90104
Invercargill 9840

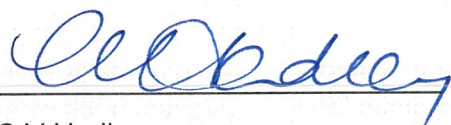
Revision History:

Reference Number:	A2160977
Effective Date:	October 2021
Review Period:	This Policy will be reviewed every three (3) years, unless earlier review is required due to legislative changes, or is warranted by another reason requested by Council.
Supersedes:	
New Review Date:	October 2024
Associated Documents / References:	Births, Deaths, Marriages, and Relationships Registration Act 1995 Public Records Act 2005 Privacy Act 2020 Local Government Official Information and Meetings Act 1987
Policy Owner:	The Manager – People and Capability is responsible for the development, maintenance and implementation of this policy.

Date:

20.10.21

Authorised By:



C V Hadley

Chief Executive

Appendix A

Privacy Principles

Principle 1

Purpose of collection of personal information

Personal information must not be collected unless -

- It is collected for a lawful purpose connected with a Council function or activity; and
- the collection is necessary for that purpose.

If the defined collection purpose does not require the need for an individual's identifying information then Council will not collect this information.

Principle 2

Source of personal information

Personal information must be collected directly from the person concerned unless:

- the information is publicly available, and the information is collected from the public source; or
- the person concerned has authorised collection from someone else; or
- non-compliance is necessary:
 - i. to avoid prejudice to the maintenance of the law; or
 - ii. for the protection of the public revenue; or
 - iii. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
- compliance would prejudice the purposes of collection; or
- compliance is not reasonably practicable; or
- the information:
 - i. will not be used in a form that identifies the person concerned; or
 - ii. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 3

Collection of information

Before personal information is collected from the person concerned (or if that is not practicable, as soon as practicable after the information is collected) reasonable steps must be taken to ensure that the person is aware of -

- the fact that the information is being collected; and
- the purpose for which the information is being collected; and
- the intended recipients of the information; and
- Council's name and address; and

- if the collection of the information is authorised or required by law -
 - i. the law authorising or requiring; and
 - ii. whether or not the supply of the information is voluntary or mandatory; and
- the consequences if the information is not provided; and
- the rights of access to, and correction of, personal information provided by the principles.

Council is not required to take the steps referred to above (of Principle 3), if Council has taken those steps on a recent previous occasion when collecting the same (or similar) information.

Compliance with Principle 3 is not required if Council believes, on reasonable grounds that -

- non-compliance is necessary -
 - i. to avoid prejudice to the maintenance of the law; or
 - ii. for the protection of the public revenue; or
 - iii. for the conduct of proceedings before any court or tribunal; or
- compliance would prejudice the purposes of collection; or
- compliance is not reasonably practicable; or
- the information -
 - i. will not be used in a form in which the person concerned is identified; or
 - ii. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4

Manner of collection of personal information

Personal information will not be collected by -

- unlawful means; or
- means that, in the circumstances of the case -
 - i. are unfair; or
 - ii. intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5

Storage and security of personal information

Members and staff must ensure that:

- personal information is protected by security safeguards that are reasonable in the circumstances against -
 - i. loss; and
 - ii. access, use, modification, or disclosure, except with Council's authority; and
 - iii. other misuse; and
- if it is necessary for personal information to be given to a person in connection with the provision of a service to Council, then everything reasonably within Council's power will be done to prevent unauthorised use or disclosure of the information.

Principle 6

Access to personal information

Where an individual makes a request for information about themselves, it must be dealt with in accordance with the Privacy Act 2020. Other requests for personal information, such as a request made by a third party, must be dealt with under the LGOIMA (refer to section 10 of LGOIMA).

Reasonable assistance must be provided to the individual to make the request (section 42 of the Privacy Act 2020). No charge may be imposed for processing and making personal information available unless authorised by the Privacy Commissioner (section 66 and 67 of the Privacy Act 2020). Where an urgent request is made, the requester must state the reason. The reason for urgency must be considered when determining priority and responding to the request (section 41 of the Privacy Act 2020).

Unless the request is to be transferred (see below) a response must be provided within 20 working days of receiving the request (section 44 of the Privacy Act 2020). The response must notify the requester that:

- the information is held, or not, and if held, access is granted or declined in part or whole; or
- the information is held but is not readily retrievable; or
- the information is not held; or
- whether the information is held, is neither confirmed nor denied.

Where information is not provided, reasons in terms of the Privacy Act 2020 must be included along with:

- supporting grounds (required unless an exception applies if requested or where the information is evaluative material); and
- information on how the requester may make a complaint to the Privacy Commissioner (section 46 and 47 of the Privacy Act 2020).

Where it is proposed that a request is declined because the information is not readily retrievable, a number of factors will be relevant including the amount of time, and cost, required to retrieve the information and the manner in which the relevant information is stored. Where there are good information storage systems in place, Invercargill City Council can only be asked to go so far. If it is not realistic to retrieve the information, then the information is not readily retrievable.

Where access to the information is to be provided, the response must inform the requester:

- how and when this will occur (section 45 of the Privacy Act 2020); and
- that they may request the correction.

Steps must be taken to identify the requester before access to the information is provided. Steps required will depend on the number of factors including:

- whether the information would otherwise have been released if requested by a third party under LGOIMA; and
- the nature of the information including degree of sensitivity; and
- the likely consequences of release to the wrong person.

Where documentary evidence is required or desirable, a copy will be saved as a record.

Where the requester is an agent for the individual concerned, the agent must provide adequate written evidence of their identity and evidence that they are authorised to obtain the information, copies of which will be saved as a record.

Where a request is made for personal information by the person concerned and the information is not held but is believed to be:

- held by another agency; or
- more closely connected to the functions or activities of another agency; then

- the request must be transferred within 10 working days of receipt and the requester informed (section 43 of the Privacy Act 2020).

Access to personal information may be refused if disclosure would, amongst other things (section 53 of the Privacy Act 2020):

- involve the unwarranted disclosure of the affairs of another individual or deceased person;
- prejudice the maintenance of the law;
- breach legal professional privilege;
- disclose a trade secret or be likely to unreasonably prejudice the commercial position of the person who supplied, or is the subject of, the information, provided these reasons are not outweighed by other considerations that make it desirable, in the public interest, to make the information available.

Access may be refused where the information is evaluative material (section 50 of the Privacy Act 2020):

- and disclosure would breach an express or implied promise made to the supplier of the information that the information or the identity of the supplier, or both, would be held in confidence;
- made available by an agency to another agency and the other agency refuses in accordance with a. above.

Evaluative material is defined as evaluative or opinion material compiled solely for the purpose of:

- determining the suitability, eligibility, or qualifications of the individual to whom the material relates for employment, appointment to office; or promotion or continuance in employment or office; or removal from employment or office; or
- for the awarding, continuance, modification or cancellation of contracts, awards, scholarships, honours, or other benefits; or
- for the purpose of deciding whether to insure, or to continue or renew insurance.
- It does not include material described above compiled by a person employed or engaged by an agency in the ordinary course of their duties (section 50(2) (b) of the Privacy Act 2020).

Access to personal information may be refused if, amongst other things (section 49 of the Privacy Act 2020):

- disclosure would be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety; or
- disclosure would create a significant likelihood of serious harassment of an individual; or
- disclosure would include information about another person who:
 - i. is the victim of an offence or alleged offence; and
 - ii. would be caused significant distress, loss of dignity, or injury to feelings; or
- the individual concerned is under the age of 16 and the disclosure would be contrary to their interests.

A request may be declined if disclosure would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand (section 51 of the Privacy Act 2020).

Information must be provided to the requestor in the manner they prefer unless an exception applies under section 56 of the Privacy Act 2020 including impairing the efficient administration of Invercargill City Council.

Principle 7

Correction of personal information

An individual may make a request for information about them to be corrected. Information must be corrected if it is reasonable to do so, having regard to the purposes for which the information may be used, to ensure the information is accurate, up-to-date, complete and not misleading. Where a requested correction is not made, if the person concerned requests, the request for correction must be attached to the information, and, so far as is reasonably practicable, every person to whom the information has been disclosed must be informed.

Principle 8

Accuracy of personal information to be checked before use or disclosure

Information must not be used without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

Principle 9

Agency not to keep personal information for longer than necessary

Personal information must not be kept for longer than is required for the purposes for which the information may lawfully be used.

Principle 10

Limits on use of personal information

Personal information obtained in connection with one purpose must not be used for any other purpose unless:

- the information is publicly available and its use is not unfair or unreasonable;
- authorised by the individual concerned;
- non-compliance is necessary to avoid prejudice to the maintenance of the law or the conduct of proceedings;
- necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual;
- the other purpose is directly related to the purpose in connection with which the information was obtained;
- the individual concerned is not identified or the information will be used for statistical or research purposes that will be published in a form that does not identify them.

Principle 11

Limits on disclosure of personal information

Personal information must not be disclosed to a third party unless:

- disclosure is required or authorised by other legislation such as the Local Government Official Information and Meetings Act 1987 (refer to section 24 of the Privacy Act 2020); or

- disclosure is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
- the information is publicly available and its intended disclosure is fair and reasonable; or
- authorised by the individual concerned; or
- non-compliance is necessary to avoid prejudice to the maintenance of the law or the conduct of proceedings; or
- necessary to prevent or lessen a serious threat to public health or safety or the life or health of an individual; or
- the individual concerned is not identified or the information will be used for statistical or research purposes that will be published in a form that does not identify them.

Principle 12

Disclosure of personal information outside New Zealand

Subject to exceptions relating to the maintenance of the law and protection of individual and public safety, personal information may be disclosed to a foreign person or entity (refer to section 7 of the Privacy Act 2020 for the definition) only if:

- authorised by the person concerned after they are informed that the information may not be subject to the same degree of protection as provided by the Privacy Act 2020; or
- the foreign person or entity is carrying on business in New Zealand and is subject to the Privacy Act 2020; or
- the foreign person or entity is subject to safeguards comparable with the Privacy Act 2020; or
- the foreign person or entity is a participant in a binding scheme or is subject to the privacy laws of a prescribed country as those terms are in section 22 of the Privacy Act 2020; or
- the foreign person or entity is otherwise required to provide comparable safeguards to those in the Privacy Act.

Principle 13

Unique identifiers

Unique identifiers may only be assigned to an individual where it is necessary to carry out Council functions efficiently. Except where two agencies are associated as defined in this part of the Privacy Act 2020, or the identifier is used only for statistical or research purposes, Council must not assign an individual a unique identifier assigned by another agency. Before unique identifiers are assigned, reasonable steps must be taken to clearly establish the individual's identity