PRIVACY (PERSONAL INFORMATION) POLICY

1. Introduction

This Policy aims to help Council effectively manage privacy breaches of personal information.

A "privacy breach" generally refers to unauthorised or accidental access to, or disclosure, alteration, loss or destruction of, personal information. It also captures situations where Council cannot access its information, either temporarily or permanently.

Privacy breaches are generally recognised as one of the more costly security failures of organisations. They can lead to significant reputational and financial losses.
Council uses and stores a variety of personal information in conducting its business and the utmost care should be taken at all times with how this information is treated. This Policy outlines the actions to be taken should a privacy breach occur.

2. Scope

This Policy applies to all employees, members (elected and appointed), and to any appointed "officers" of the Council who are directly employed by a contractor to the Council (such as Nelmac or Environmental Inspections Limited). Every role of Council must be familiar with this policy and comply with its terms.

This Policy also applies to volunteers and contractors where they are acting as an agent of Council.

For ease of reference, the term "workers" will be used to encompass all the roles above that fall within scope of the policy.

3. Personal information

This Policy concerns privacy breaches of "personal information" that is held by Council.

The Privacy Act 2020 defines personal information as "Information about an identifiable individual".

Personal information is information that concerns an "individual", ie a real person. Companies and other entities do not have "personal information" that is protected under the Privacy Act.

To be "personal information", information does not need to be especially private or sensitive – it can be any information that relates to a person, however innocuous, and

even if it is already known to others (e.g. the fact that a particular individual owns a dog is their personal information).
Most commonly, an individual will be "identifiable" from information because their name is included. However, even if someone's name is not included, the information may still be "personal information" if it is possible to identify the individual concerned from that information, perhaps by combining it with information known to others (e.g. reference to the "resident at 12 Short Street" is sufficient to identify the individual and make that information "personal information", without mentioning their name).

Aggregated information, where all identifying information has been removed, is not personal information.

4. Privacy Officer

The Privacy Act requires that every agency have a Privacy Officer. The Privacy Officer is responsible for:

- Ensuring Council complies with the Privacy Act
- Addressing requests for access to, or correction of, personal information
- Working with the Privacy Commissioner on investigation of complaints

Part of ensuring compliance with the Privacy Act includes responsibility for the internal investigation of any privacy breaches. Such investigation will ensure appropriate actions are taken to manage the particular incident and will also contribute to helping prevent future privacy breaches.

Council's Privacy Officer is the Group Manager, Strategy and Communications.
The Manager Governance and Support Services acts as a delegate for the Privacy Officer.

5. Privacy breaches and their causes

In the Privacy Act 2020, a "privacy breach" is defined as meaning:

- unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information; or
- an action that prevents Council from accessing personal information on either a temporary or permanent basis.

The definition makes clear that these actions will be privacy breaches whether or not they are ongoing, caused by a person inside or outside Council, or attributable in whole or in part to the Council.

In practice, privacy breaches are most often caused by people (either within Council or external parties) or technology errors. Some examples of possible privacy breaches are listed below.

Human Error
Human error causes include:

- Loss of computing devices (portable or otherwise – for example PCs, laptops, tablets, iPads and phones), data storage devices, or paper records containing personal data
- Disclosing information to the wrong recipient
- Handling information in an unauthorised way (e.g. downloading a local copy of personal data)
- Unauthorised access or disclosure of personal data by employees (e.g. sharing a login)
- Improper disposal of personal information (e.g. hard disk, storage media, or paper documents containing personal information sold or discarded before information is properly deleted)

Malicious Activities
Malicious causes include:

- Hacking incidents / illegal access to systems containing personal information
- Theft of computing devices (portable or otherwise), data storage devices, or paper records containing personal information
- Scams that trick workers into releasing personal information

Computer System Error
Computer System Error causes include:

- Errors or bugs in an application
- Failure of cloud services, cloud computing or cloud storage security / authentication / authorisation systems

6. Responding to a Privacy Breach

Workers must report any confirmed or suspected privacy breaches **AS SOON AS POSSIBLE** to the Privacy Officer by phone and follow that up in an email report.

Where the worker is a volunteer or contractor, they must also notify their Council liaison/ contract manager that an issue has occurred, and that they have contacted the Privacy Officer. The Council liaison may be required to work with the worker on the email report.

Time is of the essence in addressing privacy breaches. Noting that the Privacy Officer may not be immediately available, their delegate may also be contacted.

Privacy Officer: **Group Manager Strategy and Communication**

Delegate: **Manager Governance and Support Services**

The email report should include the information outlined in the "Assess Risks and Impact" section of the Privacy (Personal Information) Breach Management Plan

After receiving a report of a confirmed or suspected privacy breach, the Privacy Officer or their delegate should immediately activate the Privacy (Personal Information) Breach Management Plan This Plan addresses the stages of investigating a privacy breach, and the roles of the Privacy Officer/ their delegate and workers during those various stages.
It also addresses when a privacy breach should be notified to the Privacy Commissioner, CERT NZ (if relevant) and affected individuals.

7. Register of Privacy Breaches and Near Misses

The Privacy Officer/ their delegate will maintain a register of privacy breaches and near misses (i.e. situations that very nearly became privacy breaches).

Workers must report any near misses to the Privacy Officer or their delegate as soon as possible (as well as reporting any confirmed or suspected privacy breaches under section 6 above).

The register will help the Privacy Officer carry out their duties more effectively through providing information about problems and risks in Council, enabling the Privacy Officer to consider how best to prevent any future privacy breaches.

The register will include:

- A unique reference number for the incident
- Date of the incident
- How the incident was reported to the Privacy Officer
- Whether the incident was a privacy breach or a near miss
- Containment measures taken (if any)
- Number of impacted/potentially impacted individuals (recorded in a form in which the individuals concerned are not identified)
- Notifications made by Council (if any)
- Source/cause of breach or near miss
- Review outcomes (if any)

8. Policy compliance and review

All Council workers must observe this policy. Failure to comply puts both the worker and Council at risk.
Non-compliance with this Policy may result in conduct review processes being initiated for staff, a Code of Conduct complaint for members, and contract implications for Council contractors.

The Privacy Officer will review the Policy and Plan at regular intervals to ensure it is still fit for purpose.