Attachment C

Draft Privacy Policy

Overview

This privacy policy describes the personal information that the Council collects from and/or about employees, how it is used and whom it is disclosed to.
It also describes the behaviour expected of employees when they are using, storing or managing information in the Council's information systems so that Council complies with its obligations under the Privacy Act 1993.

Contents

Introduction

Purpose

This policy has been developed in order to communicate the Council's need to use, manage and store personal information about our employees and business units in a manner consistent with employees' privacy rights. This policy is intended to be consistent with the obligations set out in the Privacy Act 2003.

Scope

This policy applies to:

- All employees and former employees of QLDC;
- Any person seconded to QLDC;
- Any person engaged or contracted under a contract for services to do work with QLDC;
- Any volunteer delivering works or services for QLDC.

For the purposes of this document the terms 'employee' and 'employees' include all of the above.

Privacy Policy

Associated documents

Other documents that are relevant to the contents of this document are:

Type	Title
QLDC Corporate	Conflicts of interest register Protected Disclosures Policy Staff Handbook Code of Conduct Employee records policy Drug and Alcohol Policy Gifts and Hospitality Vehicle Use Policy Discipline and Dismissal Policy
Legislation	Human Rights Act 1993 Unsolicited Electronic Messages Act 2007 Privacy Act 1993 Public Records 2005 Employment Relations Act 2000 Holidays Act 2003 Tax Administration Act 1994
Other	Not applicable

Privacy Policy

Policy

Principles

The Council is an agency that is required to give effect to the Privacy Act 1993. The principles of the Privacy Act 1993 can be found in Part 2 of the Privacy Act 1993.

The Council has obligations to manage information about employees and elected members appropriately.

Employees at Council must perform their duties honestly and impartially and avoid any personal, financial, legal or professional situations which might compromise their integrity or otherwise lead to a conflict of interest.

Privacy Officer

The Council's privacy officer is the Senior Solicitor.

All requests pursuant to the Privacy Act 1993 and all questions regarding privacy issues must be directed to the privacy officer in the first instance.

PART 1 – EMPLOYEE INFORMATION

Personal Information Collected

The Council collects and retains different types of personal information in respect of those individuals who seek to be, are, or were employed or engaged by the Council, including the personal information contained in:

- Resumes/CVs;
- Applications for employment and supporting documentation;
- References;
- Interview notes;
- Offers of employment;
- Council policy acknowledgment forms;
- Payroll information, including but not limited to IRD numbers and tax codes, bank account details for wage / pay deposit etc.;
- Psychometric testing results;
- Pre-employment checks, including but not limited to health checks, police vetting forms and NZTA forms;
- Health and safety forms relating to benefits, long and short term disabilities, medical care and emergency contact information;
- ACC information;
- Performance assessments and agreements;
- Evaluative information associated with restructuring;
- Disciplinary information (including health checks).

In addition to the examples above, personal information also includes information such as full names, residential addresses, telephone and mobile number(s), personal email addresses, dates of birth, employee identification numbers for people management software as well as any other information necessary to enable the Council to meet its obligations as an employer.

Personal information will be sought wherever possible directly from the individual concerned, unless the employee agrees otherwise.

Use and disclosure of personal information collected

The Council may share employees' information with other Council employees, consultants and other parties who require such information to assist the Council with establishing, managing or terminating the Council's employment relationship with its employees, or for purposes associated with the Protected Disclosures Act 2000.

The Council must comply with Privacy Principle 11 of the Privacy Act 1993 which provides that information should not be disclosed to third parties unless:

- The disclosure is directly related to the reason the information was collected in the first place;
- The employee has authorised the disclosure;
- The information is publicly available;
- Disclosure is necessary for the maintenance of the law or for legal proceedings (e.g. for the Employment Relations Authority); or
- Where possible criminal or other unlawful activity is suspected.

The Council is subject to the Local Government Official Information and Meetings Act 1987. Information may not be disclosed if the grounds in section 6 or section 7 apply.

Privacy Policy

Protection of Personal Information

The Council endeavours to maintain physical, technical and procedural safeguards that are appropriate to the sensitivity of the employees' personal information. These safeguards are designed to prevent personal information from loss and unauthorised access, copying, use, modification or disclosure. These include:

- Keeping employees' personnel files in hardcopy which is stored under lock and key, and restricting access.
- Limiting access to employees' personal information on its electronic systems by restricting access.

Employees are requested to sign a consent form which permits the storage and collection of employment information.

Employee files are stored in a locked area, and access to the locked area is restricted and monitored.

It is important that the information held in Council records is both accurate and current. If an employee's personal information changes during the course of their employment the online form "Employee Amendment Form" should be completed, together with the "My Details" area of "My HR" the Council's Human Resource software system.

If an employee believes that the information held by the Council about him or her is incorrect, the employee in the first instance should request the record holder to correct the information. If the information is not corrected, the employee may make a written request to the Council's privacy officer to correct the information.

If the Council does not agree that the information is incorrect, the employee may have attached to that information a written statement from the employee as to what they believe the correct information to be.

Privacy Policy

Access to personal information

All employees may request to see their employee file held by HR. They should contact their HR Advisor to arrange a suitable time to do so.

Council employees can request access to their personal information verbally or in writing. Written requests are preferable. Employees do not have to explain why they want to view their information, though it is often helpful to do so. If the request is urgent, the employee must specify why it is urgent.

The Council will decide whether to agree to the request as soon as possible (20 working days is the maximum period unless an extension has been advised). The Council will provide access to the information in the way preferred by the employee unless this would impair efficient administration, breach a legal duty, or breach an interest protected by one of the withholding grounds under the Act, which the Council would then give reasons for the decision. The Council will provide access without undue delay and will give reasons for a decision to withhold information.

Employees will be able to view and copy their personal information with an HR representative present.

Employees are entitled to all other personal information held by the Council about them, including (but not limited to) their wage and time records, holiday and leave records and information held by their managers (whether in written, electronic or other form).

The Council may withhold information pursuant to Part 4 of the Privacy Act 1993, or Local Government Official Information and Meetings Act 1987. The reasons for which information may be withheld include, but are not limited to, the following:

- Giving access to information would involve the unwarranted disclosure of personal information about another person or employee;
- The information is protected by legal professional privilege; or
- Giving access to the information could hinder an investigation into a criminal offence.

Video Surveillance

The Council may operate overt video cameras in areas where criminal activity and/or actions detrimental to health and safety could occur. Camera systems may also operate for the purpose of monitoring the behavior of the public in areas where employees undertake their duties (e.g. car parks, reception areas).

Where cameras are installed for the purpose of detecting criminal activity, employees within the area of surveillance will be advised before cameras are put in and they will be advised of the purpose of the camera. Appropriate signage will be displayed.

Camera systems are on a network so that images can be accessed and these images are then stored on electronic media in a secure location.

Images of employees from any camera system may be used by the Council in disciplinary processes, health and safety investigations, to defend against a personal grievance or other court action against the Council, or for disclosure to the Police or other law enforcement agencies for the purposes of possible criminal investigations.

Stored video images will only be accessible to those persons approved by the Chief Executive. Images will be stored for approximately 25 days, but may be retained for longer periods for the purposes described above.

Images of employees will only be released to third parties in accordance with the Privacy Act 1993 for the purposes described in this clause. The prior authorisation of the Chief Executive in respect of the release of footage will be required.

Images may be used for the purposes of disciplinary action, health and safety investigations and/or disclosure to the Police or other law enforcement agency. Access will be limited to the Chief Executive, HR Manager the appropriate General Manager and Council's lawyers. Information gathered may be released to third parties in accordance with the Privacy Act 1993 for the purposes described in this policy.

Call Monitoring

Call monitoring may put in place for training purposes and complaint resolution to ensure that service delivery expectations are being met.

Staff will be advised of the commencement of call monitoring.
Incoming calls may be recorded. All outbound calls made through the desk phones may also be recorded. Call log details such as time of call, call duration and destination or source telephone number(s) are also recorded.

The Chief Executive and the General Manager of Operations and the Chief Information Officer have access to the recordings as well as screen shots to support the calls that are monitored. These recordings are stored for between 3-6 months. This information may be used for the purposes of training, health and safety, reporting potential criminal offending and managing employees' performance. Employees may request to listen to a recorded call.

Privacy Policy

GPS

The Council operates GPS devices in all vehicles. Data gathered by the Council includes vehicle routes, locations visited, speed of the vehicle at any time during the journey and the speed limit of the road being driven. This information may be used for the purposes of managing work distribution, health and safety, disciplinary purposes, or in the investigation of criminal offences. Information may only be accessed by Managers, HR Manager, the Chief Executive and the relevant General Manager. These records will be retained by the Council and may be given to third parties for the purposed described in this policy.

Door Monitoring

Entry to Council buildings may require use of an electronic swipe card. Employees are provided with a swipe card or electronic key for access to Council buildings. Swipe cards or electronic keys must not be shared between employees and must never be given to an external party. Records are kept of the time of access and the identity of the swipe card. Lost or stolen or swipe cards must be reported to an IT support technician in Knowledge Management.

Electronic Information Systems

Council employees are provided with access to computerised information and tools, usually via a personal computer, so they can carry out the duties required.

Employees are assigned a system ID. That employee is accountable for use of their system ID and therefore should not disclose their system password to any other person in Council except in exceptional circumstances and never to an external party.

Email and Internet

The Council sets out the conditions under which employees may use e-mail and internet services and these are described in the QLDC's employee handbook. It is acknowledged that personal use of the internet may occur where that does not disrupt the delivery of Council services.

These services have been installed to help employees carry out their work and employees are encouraged to make full use of them for this purpose. However, they can be used in ways that put at risk the availability of computer services, the integrity of council information and the credibility of the Council as a public organisation. The Council reserves the right to:

- Monitor, intercept, inspect and if necessary disclose e-mails transmitted by, received by, or stored using Council computers or equipment;
- Monitor and if necessary disclose the history of Internet and World Wide Web pages and sites accessed using Council computers or equipment.

Privacy Policy

Monitoring activity will be to the extent necessary to protect Council's interests and those of its employees in light of its legal obligations, to maintain business continuity, and to ensure the effectiveness of the Council's policies on electronic media and systems.

Knowledge Management installs software to detect and intercept suspected unacceptable material and to block access to web sites which have been classified as known to contain unacceptable material. When such material is detected and a release request made, the ICT Systems Team Leader will verify whether unacceptable material has been accessed or transmitted. Intercepted material found to be acceptable will be released to the recipient.

Monitoring and inspection of past usage of e-mail and internet services will be undertaken:

- On a periodic basis as arranged by the Manager HR to monitor the operation of electronic media or devices policies;
- At the request of a Manager or General Manager if there is good reason to suspect unreasonable or prohibited use of e-mail or internet services, or if responding to a legitimate request to do so by a third party;
- By Knowledge Management administrators as necessary to maintain operational effectiveness and the overall safety and security of the system.

Knowledge Management will maintain an audit trail of all Internet transactions.

Knowledge Management will bring to the attention of the Chief Information Officer any activity, which could be indicative of unreasonable or prohibited use of email or internet services.

Privacy Policy

Applicant Information

Information collected about applicants (internal or external) during a recruitment process is treated in strict confidence. This confidence extends to applications, interviews and all selection and related administration processes. Hiring managers are to ensure the interview panel are aware of this requirement.

Information regarding successful candidates is securely stored electronically and is viewable only by certain groups in the Council's Human Resources Group and the recruiting departmental managers. Unsuccessful applicants' information is retained for a total of 12 months and then destroyed. The reason for this is that this is the timeframe for an unsuccessful applicant making a complaint pursuant to the Human Rights Act 1993.

This information includes Application Forms, CV's, Interview Notes and Pre-Employment Screening, Psychometric testing, qualification checks, eligibility to work in New Zealand, health and safety assessments, health information and any Police or Ministry of Justice background checks carried out and other evaluative material.

Retention of Personal Information

The Council will retain employee's personal information after the termination of the employment relationship as required by the Public Records Act 2005, the Employment Relations Act 2000, the Holidays Act 2003 and the Tax Administration Act 1994.

PART 2 – INFORMATION IN THE WORKPLACE

Information Devices

Local government, by law, operates in a very open, accessible environment. All information held on devices, the network, whether in private file space or in shared file space, is potentially legally available to the public, unless there are reasons, as defined by statute, for withholding it.

Employees must ensure that devices are protected or locked by appropriate passwords so that in the event of theft or loss, the information can not be accessed.

Employees must never place information on the network or their computer that would embarrass or discredit themselves, other staff members, or the Council should any member of the public gain access to it. This includes e-mail messages.

Information received or created in the course of performing duties belongs to the Council irrespective of what device it is stored or used on, and who owns the device.

Taking Information Outside the Workplace

When using a Council laptop or other electronic device for work off site, users have access to Council's standard office programmes, their own personal space on the network and access to shared space on the network as required.

Users must seek advice from their manager if issues of public access to information arise, or are likely to arise.

Taking Council Documents offsite

Original corporate records must not leave Council premises. Only copies of files are to be taken offsite, they have to be marked 'copy' and destroyed after their purpose has been fulfilled.

- Any exceptions need to be approved by the one-up manager and Records Advisor.
- It is preferable for external persons to view the file in supervised conditions on site.

Records which are considered to have reduced activity or reduced direct current business value, including closed parts of files, are to be transferred at appropriate times to offsite storage. The transfer of records to offsite storage is managed by the Records Advisor and the Knowledge Management Team.

Privacy Policy

Unsolicited Messages

The Unsolicited Electronic Messages Act 2007 provides that when the Council sends commercial messages it must have the consent of the people to whom it is sending the message. It is up to the Council to be able to prove that it has the person's consent. Consent can be:

- express (e.g. ticking a box on a website to have a newsletter sent to them);
- deemed (e.g. the Council could send emails about an event at the Art Gallery to commercial/business art galleries that have published their work email addresses in advertising brochures and have not stated that unsolicited messages are not to be sent to that address); and
- inferred (when a person has not directly instructed the Council to send them a message, but it is clear there is a reasonable expectation that messages will be sent – it may be possible to infer consent of persons on existing address lists who have not 'unsubscribed', depending on the length of time over which the Council has been sending emails to the person, and how it came about that the Council is sending the emails. The Department of Internal Affairs (DIA) suggests that if an organisation is not confident that the existing relationship between the organisation and the email recipient is strong enough to infer consent, it should obtain express consent from that person).

Where the Council has a recipient's consent then it is not sending unsolicited commercial electronic messages (spam). However, it needs to ensure that such emails accurately identify the Council/Council Unit, as the sender of the message (this does not necessarily need to include an individual's name), and that the message includes a functional unsubscribe facility, to enable the recipient to advise the Council that no further messages are to be sent to the recipient. If the Council does not have a person's consent to send a commercial electronic message then it needs to obtain consent first. The Council can communicate with that person by a means other than email or text message to seek consent, or it could send an email or text to the person to seek consent, provided the email does not contain any other links or information of a commercial nature.

Privacy Policy

P-Card

P cards (Purchasing Cards) are issued to authorised employees for purchasing low value goods and services on behalf of Council. Among other principles that must be adhered to when using a P-Card (which can be found in the P-Card Policy) P-Card users must be careful around P-card security.

Care must be taken when using the internet to make a P Card purchase. Cardholders must use all reasonable care to prevent fraudulent use of Council P Cards. Cardholders must:

- Ensure any website used for purchasing is secure (https) and from a reputable source;
- Not disclose credit card number and expiry dates over email;
- Not disclose PIN number under any circumstances.

Local Government Information And Meetings Act 1987

Requests under the Local Government Official Information and Meetings Act 1987 (LGOIMA) are requests made to Council pursuant to legislation requiring disclosure of information held by the Council.

If the request relates to information that is controversial, complicated (requires large amounts of time to compile the answers) or is from the media, then this is be referred to the Records Manager. The Records Advisor will make a decision on whether it is treated as a formal LGOIMA request. The Records Advisor may also seek advice from the Senior Solicitor or General manager Legal and Regulatory or contact the Communications Manager for assistance.

Under the Local Government Official Information and Meetings Act 1987 there are acceptable reasons for refusing, or withholding information from, requests made for information. The Council's Senior Solicitor will advise on this if requested.

Information Browsing

Much of Council's information is confidential or sensitive. Use (including viewing) of information and information systems other than in the performance of employment duties is not permitted.

Employees are required to take proper care with the use, exchange or release of any information (whether written or electronic). Employees are responsible to ensure that information sent is addressed to the correct person(s) and that information remains secure at all times and is only used for its intended purpose.

Release of information and access to or handling of personal information about any individual is governed by the Local Government Official Information and Meetings Act 1987 and the Privacy Act 1993. This means

that employees must not use the privilege of this access for personal use at any time or disclose to anyone outside Council.

In using the Council's electronic information systems, Council does not guarantee employee's privacy. All information, e-mails, websites, blogs etc. accessed, downloaded or otherwise using Council's systems remains the sole property of the Council and may be accessed, copied and used by the Council at any time, with or without notice to the employee.

Document Destruction

The Council uses a document destruction service. Hardcopy documents which are no longer required and are to be disposed of must be destroyed using the document destruction service if they are of a confidential or sensitive nature.

Unintended Disclosure of Information

If an employee becomes aware of an unintended release of information or transmission of information to an unintended recipient, this must be reported to their General Manager so that appropriate action to recover the information can be taken.