PRIVACY POLICY

1. Introduction

The Wellington Museums Trust, trading as Experience Wellington, must comply with The Privacy Act 1993 ("the Act") in all matters relating to personal information.

2. Definitions

Personal Information:	The definition in the Act is broad, and not limited to information that is particularly sensitive, intimate or private. The Act defines personal information as "information about an **identifiable** individual", including but not limited to, contact details, employment agreements, personnel records, payment information and any images we may hold of an individual.
Agency:	As defined in the Act, the Agency in this instance is Experience Wellington.
Experience Wellington:	includes reference to all other trading names of the organisation – Cable Car Museum, Capital E, City Gallery Wellington, Hannah Playhouse, Nairn Street Cottage, Space Place, and Wellington Museum. It also includes the New Zealand Cricket Museum which we support the operation of.
Privacy Officer:	By law, all organisations, regardless of size, must have a Privacy Officer on staff. A Privacy Officer is someone within the organisation who is most familiar with how personal information should be handled. The sponsor of this Policy document is the identified Privacy Officer for Experience Wellington.
Spam:	Under the Unsolicited Electronic Messages Act 2007 Spam is defined as unsolicited commercial electronic messages. This covers email, mobile/smart phone text messaging, instant messages and fax. It does not cover internet pop-ups or telemarketing phone calls.

3. Policy

Experience Wellington holds personal information on its staff, visitors and clients. As responsible employers and service providers, it is essential that we understand and put into practice systems and processes that comply with the provisions of The Privacy Act 1993 and also the Unsolicited Electronic Messages ('Anti-Spam') Act 2007 (UEMA).

3.1. The Privacy Act 1993 Overview

The Privacy Act 1993 applies to "personal information" as defined in section 2 above. Its central theme is that an individual should keep control over what happens to their personal information, who can have access to it, and who can communicate with them (whether electronically or otherwise).

The Privacy Act is administered by the Office of the Privacy Commissioner[1]. If an agency holds personal information, it is obliged to comply with the Act. The Privacy Act sets out 12 privacy principles that detail how agencies may collect, store, use and disclose personal information. These are summarised below.

3.1.1. The Privacy Principles

Principle 1: Personal information can only be collected with a clear purpose

Experience Wellington will ensure that the information is collected for a lawful purpose connected with a function or activity of the organisation; and that the information is necessary for that purpose.

Principle 2: Data must come directly from the individual

Personal information must be collected directly from the individual concerned. The exceptions to this are when the agency collecting the information believes on reasonable grounds that:

[1] https://www.privacy.org.nz/

- the information is publicly available; or
- the individual concerned authorises collection of information from someone else; or
- the information will not be used in a form that identifies the individual.

Principle 3: Individuals whose information is being collected must be fully informed

When Experience Wellington collects personal information directly from the individual concerned, it must take reasonable steps to ensure the individual is aware of:

- the fact that the information is being collected;
- the purpose;
- the intended recipients;
- the names and addresses of who is collecting the information, noting that Experience Wellington holds the information;
- any law governing provision of the information and that provision is voluntary;
- the consequences if all or any part of the requested information is not provided; and
- the individuals rights of access to and correction of personal information.

These steps must be taken before the information is collected or, if this is not practical, as soon as possible after the information is collected. Experience Wellington is not required to take these steps if they have already done so in relation to the same personal information on a recent occasion.

Principle 4: Personal information must be collected lawfully

Personal information must not be collected by:

- unlawful means; or
- means that are unfair or intrude unreasonably on the personal affairs of the individual concerned.

Principle 5: Storage of personal information must be secure

Experience Wellington will ensure that;

- the information is protected by such security measures as it is reasonable to take against loss, access, use, modification or disclosure; and any other misuse; and
- if it is necessary for the information to be given to a third party in connection with the provision of a service to Experience Wellington, everything reasonably within the power of Experience Wellington is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6: Personal information must be accessible on request

Where personal information is held in a way that it can readily be retrieved, the individual concerned is entitled to:

- obtain confirmation of whether the information is held; and
- have access to information about them.

Requests can also be refused, for example, if Experience Wellington does not hold the information, or if the request is frivolous or vexatious.

Principle 7: Personal information must be correctable on request

Everyone is entitled to:

- request correction of their personal information;
- request that if it is not corrected, a statement is attached to the original information saying what correction was sought but not made.

If Experience Wellington has already passed on personal information that is then corrected, it should inform recipients about the correction.

Principle 8: Accuracy of personal information to be checked before use

Experience Wellington must not use or disclose personal information without taking reasonable steps to check it is accurate, complete, relevant, up to date, and not misleading.

Principle 9: Personal information not to be kept for longer than necessary

Experience Wellington must not keep personal information for longer than needed for the purpose for which the agency collected it.

Hard copy Personnel files and pay records can be destroyed immediately after an employee leaves the organisation as long as there is an electronic copy securely filed. Electronic copies of Personnel files must be kept for at least six years, and pay records for seven years, after an employee leaves the organisation.

Principle 10: Use of personal information is restricted

Personal information obtained in connection with one purpose must not be used for another. The exceptions include situations when Experience Wellington believes on reasonable grounds that the:

- use is one of the purposes for which the information was collected; or
- use is directly related to the purpose the information was obtained for; or
- information came from a publicly available publication; or
- the individual concerned has authorised the use; or
- the individual concerned is not identified.

Permissible use can include facilitating and completing the transaction, confirming the purchase, providing information about the venue, cancelling the event, or following up about transaction or booking problems.

By contrast, promoting subsequent events by mail or telephone is not a directly related use.

It is therefore essential that, when personal information is collected, the stated purposes of collecting include subsequent provision to any/all of the relevant Experience Wellington institutions. This should be set out in the terms and conditions agreed to by the customer.

The Creative New Zealand / Arts Australia Customer Data Use Guidelines[2] contain best practice examples of terms and conditions from the sector.

There are specific occasions where the use of information for a non-notified purpose may be justified, for example, to prevent a crime or for the conduct of legal proceedings.

Principle 11: Disclosure of personal information is restricted

Personal information must not be disclosed unless Experience Wellington reasonably believes that:

- the disclosure is in connection with, or directly related to, one of the purposes for which it was obtained; or
- it got the information from a publicly available publication; or
- disclosure is to the individual concerned; or
- disclosure is authorised by the individual concerned; or
- the information is to be used in a form in which the individual concerned is not identified.

Principle 12: Use of unique identifiers is restricted

Unique identifiers – such as IRD numbers, bank customer numbers, drivers licence and passport numbers – must only assigned to individuals if this is necessary for Experience Wellington to carry out its functions efficiently.

3.1.2. Responding to a Data Breach

If you become aware of a data breach – eg the data storage system gets hacked or personal information is accidentally lost or released – the following steps must be taken as quickly as possible to minimise harm to those people affected and to protect the reputation of Experience Wellington:

3.1.2.1. Contain the Breach and Make the First Assessment

Once you discover a breach, immediately contain it and notify Experience Wellington's Privacy Officer. You can contain the breach by stopping any unauthorised practices, disabling the breached system, cancelling or changing computer logins, or trying to get the lost information back. Along with Experience Wellington's Privacy Officer, complete an initial investigation of the breach and make recommendations, this may include seeking advice from IT or legal experts.

[2] http://www.creativenz.govt.nz/assets/paperclip/publication_documents/documents/307/original/customer_data_access_guidelines.pdf

Experience Wellington's Privacy Officer, in consultation with the Chief Executive may decide to notify the New Zealand Police at this point if the breach appears to involve theft or other criminal activity.

3.1.2.2. Evaluate the Risks

Assessing the risks of the breach will help determine next steps. Consider:

a. What type of personal information was involved? (The more sensitive the information the higher the risk of harm to those affected).
b. What might be shown by the personal information?
c. Is the personal information easy to get at? (Does the information have encryption or password protection?)
d. What caused the breach and could it happen again?
e. What is the extent of the breach? (Try to identify the size of the breach)
f. What is the potential harm of the breach?
g. Who holds the information now?

3.1.2.3. Notify Affected People if necessary

If a data breach creates a risk of harm to a person, you should usually notify them. Notifying them promptly means they can take steps to protect themselves and regain control of their information as soon as possible.

Do not notify people unless you are sure that the breach has compromised their information. Notifying the wrong people by mistake can cause unintentional damage.

If in doubt please refer to the Privacy Commissioner's website[3] for guidance before notifying any affected parties.

3.1.2.4. Prevent a Repeat

Following the immediate response to the breach as outlined in sections 3.1.2.1 – 3.2.2.3 above take the time to thoroughly investigate the cause of the breach and put mitigations in place to prevent a breach of this type from occurring again.

Depending on the severity and type of breach, prevention of a recurrence could include:

- Security audit of physical and technical security;
- Review of policies and procedures;
- Review of employee training practices; or
- Review of any service delivery partners caught up in the breach.

3.2. Unsolicited Electronic Messages Act 2007 Overview

The Unsolicited Electronic Messages Act 2007 (UEMA) addresses the problem of "spam". One of its core provisions is that commercial electronic messages must not be sent unless the sender has the recipient's explicit consent. All personal information gathered must be treated in accordance to The Privacy Act 1993. UEMA is enforced by the Department of Internal Affairs[4].

3.2.1. Unsolicited Electronic Messages Act 2007 (UEMA)

The UEMA Act covers email, SMS text messages, instant messaging, MMS (multimedia message services) and other mobile-phone messaging, and faxes. UEMA does not cover voice calls.

There are two important issues to be considered in relation to electronic messages:

i. **Sending of electronic messages** – UEMA requires consent for the sending of commercial electronic messages. A responsible means of gaining access to email addresses would include making subsequent use conditional on the customer's selection of "yes" in an opt-in question relating to use of personal data at the point of collection. Evidence of this choice must remain attached to the customer's record.
ii. **Consent to receive electronic messages** – Under UEMA, consent must be explicit.

Experience Wellington expects that all electronic messaging to customers follows three clear steps:

[3] https://www.privacy.org.nz/privacy-for-agencies/data-breaches/responding-to-data-breaches/

[4] https://www.dia.govt.nz/Spam-Information-for-Businesses

A. **Consent:** Electronic messaging is sent only to those who have agreed to receive it, eg they subscribed or requested information;
B. **Identify:** It is clear that the electronic message is from Experience Wellington (including the relevant trading name/visitor experience) and includes contact details for the organisation; and
C. **Unsubscribe:** The electronic message includes easy provisions for the customer to 'opt-out' of receiving electronic messages from us.

3.3. Privacy and CCTV

Because CCTV (Closed Circuit Television) captures images of people which can be used, stored, manipulated and disseminated, Experience Wellington staff need to be aware of the implications of gathering such data, and the measures that should be taken to ensure the Privacy Act is observed while retaining maximum usability of data.

Experience Wellington operates CCTV monitoring in the public spaces and front of house areas at some of its visitor experiences (currently Cable Car Museum, City Gallery Wellington, and Wellington Museum). The purpose of this monitoring is to ensure the safety of staff interacting with the public, ensure the safety of the art and artefacts we have on display, and to protect against theft in our retail and front of house areas.

In line with the guidelines set out by the Office of the Privacy Commissioner, Experience Wellington must:

- Erect signs near the CCTV Cameras and at the perimeter of the CCTV system's range which alerts visitors that Experience Wellington is operating CCTV monitoring and what the purpose of the monitoring is. This also includes placing a notice on relevant Experience Wellington websites if appropriate.
- Ensure staff are informed that if they are working in areas where CCTV monitoring is in operation they are also subject to monitoring.

Experience Wellington reserves the right to use CCTV camera footage to resolve employment disputes involving an employee, in line with the Cessation of Employment, Employment Relationships, and Discipline & Dismissal Policy (Section 14 of the Human Resources Manual).

3.3.1. Guidelines For Use of CCTV at Experience Wellington Sites

3.3.1.1. Define a Purpose and Develop a Business Plan

Define your site's need for a CCTV system, and ensure your system is set up with that as a guiding principle.

Identify the existing problem you seek to address (eg to detect and capture evidence of a crime, to actively deter crime, or to allow a quick response to emergency situations); whether CCTV could address that problem and if so, how; and whether there are other alternative options available.

Consult with staff who may be affected by the installation of CCTV if necessary.

Develop a business plan for the CCTV system which sets out the purpose of the system, the outcome/s you expect, the type of technology and equipment that will be used, how the system will be operated, and how the privacy impacts will be addressed and minimised. The business plan should be accessible to all staff for reference.

3.3.1.2. Select and Position Cameras to Minimise Risk

Choose equipment which will achieve your purpose in the most privacy-friendly way[5]. Cameras should be positioned so they won't intrude on the privacy of individuals.

3.3.1.3. Make people aware of your CCTV system

Erect signs near the CCTV cameras and at the perimeter of the CCTV system's range. The signs should make clear that Wellington City Council owns and operates the CCTV system. A full privacy notice should appear on the relevant Experience Wellington websites and be available at front of house to let visitors know more about the operation of the CCTV cameras. Staff should be able to answer any queries, or direct questions to an appropriate person.

3.3.1.4. Collect only necessary data

CCTV systems operation should be limited to key times.

[5] Note that as our buildings are owned by Wellington City Council we will manage our CCTV installation and monitoring through Council's Security Team in consultation with Experience Wellington's Buildings Manager.

3.3.1.5. Only use CCTV images for the original purpose or with consent

Images collected with CCTV cameras can only be used for the original purpose they were collected for. They cannot be publicly disclosed unless you have the consent of the individual(s) shown in the footage, or after consultation with the Police.
As the CCTV footage collected from Experience Wellington sites is owned by Wellington City Council, access to footage for situations which require Police involvement (such as theft) will be obtained by the Police directly from Council's Security Team via a Local Government Official Information and Meetings Act (LGOIMA) Request. For access to footage required as evidence in an employment dispute, the Manager People and Capability will submit the LGOIMA request to Council's Security Team and will subsequently be responsible for protecting and storing the footage in line with this Privacy Policy.

3.3.1.6. Protect, store and retain images for a specified time

CCTV images should be protected from loss, unauthorised access, use, modification and disclosure. They should only be retained for a specified time - this time period must not be longer than is necessary to achieve your purpose.

3.3.1.7. Control who can see the images

The control room should only be accessible to authorised staff. Procedures must be in place for individuals that wish to access images of themselves, and for when and how you disclose CCTV images to the Police. Maintain a log of all access to CCTV images by external parties.

3.3.1.8. Regular system audit and evaluation

At regular intervals, the operation of the system should be evaluated to determine its effectiveness; its continuing viability; and to ensure that staff or CCTV operators are complying with policies.

4. The Role of the Privacy Officer

The duties of the Privacy Officer include:

- Developing good policies for handling personal information that suit your business's needs.
- Handling queries or complaints about privacy from customers or employees.
- Alerting you to any risks to personal information, eg careless handling or cyber attacks.
- Liaising with the Office of the Privacy Commissioner if necessary.
- Providing advice to managers on how to ensure compliance with the Privacy Policy.

If something goes wrong, the Privacy Officer should be the first point of contact to review the situation, provide advice and help respond to privacy-related complaints.