PRIVACY POLICY AND GUIDELINES

Privacy Policy

The Wellington Museums Trust (trading as Experience Wellington and herein referred to as "the Trust") is an agency for the purposes of The Privacy Act 1993. This means that the Trust must comply with The Privacy Act 1993 ("the Act") in all matters relating to personal information.

The definition of "personal information" 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".

The Trust holds personal information on its staff, visitors and clients. Please note that personal information **INCLUDES** any images we may hold. 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 1993 Privacy Act and also the 2007 Unsolicited Electronic Messages ('Anti-Spam') Act (UEMA). Sources of support are detailed below.

For Further Information

The following guidelines provide general information about the Privacy Act and UEMA. They are not a legal analysis. If you need more specific information, please see the Privacy Act in full, visit the website: http://www.privacy.org.nz, contact the Office of the Privacy Commissioner (0800 803 909), email enquiries@privacy.org.nz, or seek legal advice.

For an overview of the way the Privacy Act interacts with use of CCTV, see 'Privacy and CCTV: A Guide, 2009' also available on the website http://www.privacy.org.nz. It provides an overview of legal compliance and an excellent practically-focussed checklist for businesses.

In addition the Creative New Zealand/Arts Australia 2012 publication 'Customer Data Access Guidelines' provides an excellent overview of the relationship between the Privacy Act and the Unsolicited Electronic Messages Act and examples of standard terms and conditions developed by a variety of arts organisations[1].

The Department of Internal Affairs recommends that organisations seek legal advice or talk to DIA's Anti-Spam Compliance Unit if they have doubts about whether they have consent: www.dia.govt.nz/Contact-us#Anti-Spam or info@antispam.govt.nz or (04) 495 7200.

Privacy Act Overview

The Privacy Act applies to "personal" information i.e. information about an **identifiable** individual. 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. 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.

Unsolicited Electronic Messages Act Overview

The 2007 Unsolicited Electronic Messages Act (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. UEMA is enforced by the Department of Internal Affairs.

The Privacy Principles

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

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

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

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:

- 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 the Trust 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 and who will hold it;
- 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. The Trust 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

The Trust 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 the Trust, everything reasonably within the power of the Trust 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 the Trust 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 the Trust 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

The Trust 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

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

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 the Trust 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 Trust institutions. This should be set out in the terms and conditions agreed to by the customer.

The Creative NZ/ 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 the Trust 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 the Trust to carry out its functions efficiently.

Unsolicited Electronic Messages Act 2007

The Unsolicited Electronic Messages Act (UEMA) 2007 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 consent for this. All personal information gathered must be treated in accordance to the Privacy Act.

The 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:

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

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.

Privacy and CCTV

Because CCTV captures images of people which can be used, stored, manipulated and disseminated, Experience Wellington Museums staff need to be aware of the implications of gathering such data, and the measures that should be taken to ensure privacy compliance is observed while retaining maximum usability of data.

A comprehensive set of guidelines and checklist have been developed by the Officer of the Privacy Commissioner to help organisations manage their CCTV systems in line with legal constraints and good personal information handling practice[3]. The associated checklist for businesses using CCTV provides an excellent basis for assessing current systems, and is recommended as a starting point for Trust staff wishing to assess the compliance of CCTV systems and processes. An overview of the guiding principles for use of CCTV follows:

Summary of Best Practice Use of CCTV

1. Define a Purpose

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

2. Select and Position Cameras to Minimise Risk

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

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 who owns and operates the CCTV system. A full privacy notice should appear on your website(s) 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.

4. Collect only necessary data

CCTV systems operation should be limited to key times.

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.

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.

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.

8. Regular system audit and evaluation

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

[3] http://privacy.org.nz/news-and-publications/guidance-notes/privacy-and-cctv-a-guide-to-the-privacy-act-for-businesses-agencies-and-organisations/