Privacy Management at UC
Information and Records Management (IRM)

Privacy.

www.canterbury.ac.nz/irm
Privacy Management at UC

1. Introduction
Information that staff or contractors create and collect at UC needs to be managed carefully. Guidance for how this information is managed is governed by the Public Records Act 2005. The Information and records management team have a wealth of information and resources to assist UC staff in complying with the Act. Good and reliable management of information is particularly necessary for information that is considered private, sensitive, or confidential.

2. Personal or sensitive information
Private information means ‘personal information’ which according to legislation is any information about an identifiable individual. At UC this means information that is of a personal nature (such as name, date of birth, address) that could be used to identify that person—this includes photographs. Personal information also includes ‘sensitive personal information’. Sensitive personal information is typically determined by considering the potential or actual loss of dignity, humiliation or injury to feelings that would result if that information is lost, inappropriately accessed or used. Examples include health information, background or criminal records.

See a full list of the types of information collected about individuals at UC in Section 3 of the UC Privacy Policy, and about the management of sensitive personal information in Section 5.
3. Privacy Principles

Integral to managing privacy at UC are the Privacy Principles within the Privacy Act 1993. Here is a summary of what the twelve principles cover:

a. Collection of personal information

Principle 1: Purpose of collection
An agency should not collect personal information unless it is for the lawful purpose connected with a function or activity of that agency, and it is necessary to collect that information for that purpose.

Principle 2: Source of personal information
Personal information must be collected directly from the individual concerned unless the collection is believed to be an exception on reasonable grounds, such as the information is already publicly available.

Principle 3: Collection of information
During collection of personal information, an agency must take reasonable steps to ensure the individual is aware of the fact the information is being collected, for what purpose and who will use it.

Principle 4: Manner of collection
Personal information must not be collected by unlawful means or means that are unfair or intrude on the personal affairs of the individual.

b. Storage and security

Principle 5: Storage and security
This outlines the standards that organisations must meet for the accuracy, currency, completeness and security of personal information.

c. Right to access and correct personal information

Principle 6: Right to access
This outlines access rights to personal information held by an agency.

Principle 7: Correction of personal information
This gives a general right of access to have that information corrected if it is inaccurate, incomplete or out of date.

d. Use and disclosure of personal information

Principle 8: Checking accuracy of information before use
An agency must take all reasonable steps to ensure information is accurate, complete, relevant and not misleading prior to using that information.

Principle 9: Retention of personal information
An agency cannot keep information for longer than is required for the purposes for which the information may be lawfully used.

Principle 10: Limits on use of personal information
An agency cannot use information that has been collected for one purpose and use it for another purpose that was not originally specified.

Principle 11: Limits on disclosure of personal information
There are limits under which an agency may disclose collected personal information. For example, personal information must not be disclosed unless the agency reasonably believes that the disclosure is authorised by the individual and is in connection with the purpose for which it was obtained.
e. Using unique identifiers

**Principle 12: Using unique identifiers**
Unique identifier must not be assigned to individuals, unless it is necessary to enable the agency to perform its functions efficiently. This provides a safeguard against the creation of a single identifier that could be used to cross-match data across agencies.

This summary was adapted from The Privacy Commission website (www.privacy.org.nz).

---

4. Collection of Information

Information collected by UC should be collected for a specific purpose which the person knows about, and the individuals should know that the information is being collected from them and give permission for that collection and any usage.

**Student information**

When students enrol at UC, they read a declaration and agree to the information collected at this point and throughout their study to be used for the specific purposes of conducting normal and proper University business or for statutory requirements.

More information can be found on the Privacy Statements, Declaration and Agreement pages on the web: http://www.canterbury.ac.nz/privacy/

Refer to the UC ‘Survey Policy and Application Procedures for Online Student Surveys’ (see UC Policy Library) if you are thinking of doing a survey that involves requesting or collecting additional personal information or data from cohorts of students.

**Staff information**

Staff information is collected when they are hired or contracted to work for the University. The information is managed by the HR department or any other department such as UC Security (who may hold for example Parking Permit information). This information is maintained in various systems, but there is an expectation that any personal or sensitive information has restricted access and is only kept and maintained for the purposes of staff fulfilling their roles or coordinating activities related to University business.
Visitor Information

When visitor information is collected, it is important that they know that it is being collected, and why, and that they agree to this. Ensure that if you are collecting external people’s information – for example whilst arranging a conference at UC – that you follow the basic privacy principles outlined above.

Online Form collection

All online forms (for internal or external use) require privacy and consent statements. See http://www.canterbury.ac.nz/web/how/forms/ for details on your legal obligations and a link to wording you can copy and edit for privacy and consent use.

You cannot use non-university forms or systems for the collection or storage of staff or student personal data. There are some exceptions including the use of Qualtrics for the collection of survey data. If you are thinking of using an external host to capture external people’s information, then please consult with the Web Team or IRM first.

Template

A template for gaining consent to collect information is available at the back of the UC Privacy Policy (p23). Please contact records@canterbury.ac.nz for specific help and advice when using or adapting the template for your purposes.

Information should only be collected from individuals for specific purposes relating to the specific functions and business activities of UC. Any collection outside of these grounds requires specific consent from the individual whose information is being collected in alignment with Section 2.3 of the Privacy Policy. If you are in doubt about any kind of data collection at UC, please contact records@canterbury.ac.nz.

5. Use and Disclosure of Information

Be careful to follow the UC Privacy Policy in terms of how you manage the use and disclosure of personal information at UC. It must be used and disclosed for the purposes that were stated during collection. More information about this can be read in Section 2.4 of the UC Privacy Policy (see references).

There are certain circumstances where information may be able to be disclosed without consent but this is very limited. Even in a case where the Police or other Government agencies request information (including Immigration New Zealand), the Privacy Principles apply. In these cases, please contact the Registrar immediately before releasing information.

In cases of emergencies or accidents it may be reasonable to release certain information, particularly when such release is necessary to prevent or lessen a serious and imminent threat to individual or public safety. If uncertain, contact the IRM or the Registrar for advice.
6. Management and Disposal of Information

The University is subject to the Public Records Act 2005, and as such has to create and manage its records according to the Act. We have a General Disposal Authority (GDA, see link at end of this brochure) which outlines how long records need to be retained which staff must follow. In terms of private information, principle 9 of the Privacy Act states that an agency should not keep information longer than is required for the purposes for which the information may be lawfully used. This means that once you have finished using the collected information for its purpose, and as long as it is no longer needed for administration purposes under the GDA, you should dispose of the information in a secure manner. Hard copy records should be shredded or put in a locked secure destruction bin, and electronic records should be deleted from drives or file systems such as SharePoint where appropriate. See Section 4.5 of the Privacy Policy.

**NOTE:** This disposal should follow the processes outlined by the IRM Process Manual (see references).

7. Information Network

The IRM team runs an Information Network which acts as a forum to distribute advice and updates about information management, recordkeeping advice, privacy of information, and official information requests at UC. Each Senior Management Team (SMT) portfolio has delegated first line responsibility for privacy issues to a member of their team.

Monthly emails are sent out to network members, and the members are encouraged to discuss the content with their wider team and bring any queries back to the IRM team for advice. If you would like to join the Network please contact records@canterbury.ac.nz

Security of personal information

Personal or sensitive information should not be left unlocked or lying around for others to see. If you share an office, ensure you put the item away in a file and lock it in a secure cabinet. Personal information should not be carried around on USB sticks unless encrypted, and multiple instances of personal electronic information (such as database extractions) must not be copied to removable storage media or removed from secure systems. More information about this can be read in Section 4 of the UC Privacy Policy, in particular Sections 4.5 and 4.6.
8. FAQs

Here are some frequently asked questions about how to manage personal information at UC:

1. **What should I do if I accidentally supply an individual's personal information to someone who was not meant to receive it?**

   Do not panic, but the best thing to do is take action to remedy the situation immediately.
   - First, call or email the IRM team to let them know what has happened.
   - Next, contact that person that you have accidentally emailed and ask them to please delete the email they have received and any personal information attached to it. Explain the mistake and apologise for the inconvenience and state the reason for asking them to delete the information; to protect an individual’s privacy.
   - Next, call the person whose privacy has been breached, and let them know what has happened and that you have taken action to mitigate any further consequences. Apologise and explain why the incident happened and that you are putting steps in place to prevent it from happening again.
   - Then you will need to begin this process of ensuring this type of breach doesn’t happen again. The breach may be bigger than just affecting one or two people. Access and document what occurred and provide this to IRM.
   - You may need to send out a communication (with email addresses hidden/blind copied) to all of those who have been affected outlining the incident and steps being taken to prevent any issues.
   - You may also need to provide additional advice on a case by case basis. For example they may need to notify the bank if you have accidentally provided someone’s credit card information.

2. **Can I use non-UC cloud based services to store personal information?**

   No, it is wise not to use any cloud based service to store personal or sensitive information that should be held on UC servers. There shouldn’t really be any need to share personal information via the cloud, as individuals should be emailed, posted, or given their information by hand. There should be no reason to supply bulk information via the cloud. For internal sharing of personal information, SharePoint with permissions activated, or a secure drive should be used.

3. **Should I be keeping spreadsheets of personal information when I no longer need it, just in case I need it again?**

   No, you should only be holding spreadsheets of personal information for transactional reasons; e.g. to email within department or schools. Once it has been used for the purpose(s) it was collected for, it should be destroyed according to the University’s General Disposal Authority (see GDA in resources), and if approved by your manager and IRM, deleted from all locations (or shredded if printed). If you have gathered the information directly from people, it should only be collected and stored for that purpose. If you have run a report from a Student Management System or other personal data system, then that system should be considered the authoritative version of that record, and any transactional copies/cohorts of information should be deleted when no longer necessary. The reason for this is to protect inadvertent release or misuse of personal information, and also because the information may not be up to date and therefore should not be relied upon. There may be exceptions to this, so if you have any queries or concerns call IRM to have a chat, or email them at records@canterbury.ac.nz.
4. An external party asks me for some information about an individual or a group of people, should I provide it?

As a default, the answer should be no. However there are cases where we are obligated or required under legislation or contracts to provide information. This will be on a case by case basis. Staff should never provide email addresses, contact details, or any other personal information to an external party where consent has not been gained, or if they are uncertain of the purpose.

5. Can I release requested statistics about UC that contain breakdowns of age, gender, course of study, student ID, name and contact details?

Firstly, if you receive such a request, touch base with the IRM team. They handle all OIA requests for the University and will know what to do. The information might not automatically be released. It is important to protect people’s privacy when releasing statistics. There will be certain times when releasing information broken down into too many categories could cause privacy to be breached. For example if a class size was small enough and an age and gender were included, then someone might be able to figure out which data belonged to which individual. Remember to contact IRM if you are uncertain about any queries for information about the University or about staff or students.

6. How do I ensure that personal or sensitive information is kept securely?

There are some guidelines around keeping information held securely in Section 4 of the UC Privacy Policy. Staff should ensure that any information that they collect or manage at UC adheres to the Privacy Act principles outlined in this brochure, and in the Privacy Policy. Advice includes not leaving personal information lying around, on USB sticks, or on desks. Lock your computer if it is unattended. It is also wise to find ways to minimise information being lost or forwarded on to other people; this can include linking to a secure SharePoint site, encrypting data, or not forwarding on long streams of emails without considering the content at the bottom of the chain.

Generally it is advised that you use common sense and think about the information as if it was your own. How would you prefer someone to store your information? Would you like others to be able to access it who shouldn’t? Would you like it to be used for purposes other than that which it was collected for? Protect other people’s information as if it was your own.

7. Should I store information on USB sticks, or take personal information home with me to keep working on it?

No. Sensitive personal information should not be stored in uncontrolled systems or locations. To use information away from work it is recommended that this information is only accessed offsite via electronic means through University networks.

However, if it is absolutely necessary to take some information out of a business unit or college (e.g. for marking, job applications), staff must take precautions such as using encryption, password protected files, or a
locked briefcase. If taking information away from work, the information must not be left unattended at any time. All reasonable steps must be taken to ensure the information is not accessed by unauthorised people. Additionally, databases of staff or student information must not be copied to removable storage media or removed from secure systems.

8. **What is the best way to manage personal information when sending emails?**

Section 6 of the Privacy Policy provides some good information about handling of personal information to prevent breaches when using email. Email is not a guaranteed secure form of communication. At times unauthorised people may get access to emails through unattended screens, incorrect addressing, forwarding, printed emails, or hacking. Emails should not be used to send sensitive personal information unless in all circumstances it is reasonable to. Consider sending a “test email” first to ensure that the intended recipient is identified. Also consider encrypting any attachments with a password and providing the password via phone to the recipient or by independent means. Be careful when using the ‘Cc’ or ‘Bcc’. Don’t send information to individuals who do not require the information. Refer to the IRM Email Management Brochure for full information about email management at UC (see references).

9. **What kind of information can be requested under the Official Information Act 1982?**

The Privacy Act 1993 is followed when answering requests for information by an individual about themselves. However, if there has been a request by an individual for personal information about another individual then this request will be treated under the Official Information Act 1982. Emails sent or received by a University staff member might also be subject to requests for access under the Official Information Act 1982 and the Privacy Act 1993. Therefore it is wise to consider how you collect and store information about individuals as it can be provided to them, and will be unless there is good reason to withhold it under one of the relevant Acts above.

10. **Are photographs considered personal information? And what precautions should be taken when using people’s photos?**

Any identifiable information about an individual, including their photograph, is considered private information. This is anything which instructs, tells or makes another person aware of an identifiable individual. A person MUST be aware of intended uses of their personal information, especially if it is going to be used for marketing/publications/commercial activity. If consent is given it should be carefully noted and kept; use the UC Photo and Video Consent forms (available from the Student Services and Communications intranet site). Photos are considered records if they are created in the course of the University’s business transactions and day to day functioning. However photos have different retention periods dependent on what they were used for. Speak to the IRM team if you are uncertain about individuals’ privacy in photographs, or how long you need to keep them.
9. Case Studies

Access to an individual’s personal information under the Privacy Act 1993

James is a staff member who has a grievance against another staff member Tony at the University. Instead of meeting to resolve the matter, James’s manager has sent a series of emails back and forth with Tony about the matter. These emails have gotten out of hand. The matter is very serious. James has now requested under the Privacy Act 1993 to view any information that has been held about himself at the University, including email correspondence. Under the Privacy Act 1993, the University is required to provide any information that is held about the individual including emails that may discuss James. There are certain exceptions under the Act which may limit disclosure, however these are largely related to risk to the public being caused if they are released.

There seems to be no reason to withhold this information about James. When all of the information is collected and released, James sees that it contains communications between his manager and Tony which are derogatory and have ultimately inflamed the predicament and employment issues that he is now having. A dispute between James and Tony, and the University occurs. The emails lead to disciplinary action being taken against the other staff member, a personal grievance initiated by James. This is followed by an unsuccessful mediation, and then ultimately ends up in Employment Court.

**Issue:** All information held about an individual is discoverable under the Privacy Act 1993, and there are not many reasons for withholding it from the individual. Appropriate conduct has not been considered when communications have occurred, and therefore the discovery process has led to a larger dispute that could have been mediated earlier had a meeting been held between the parties instead of emails being sent back and forth.

**Risks:** Legal, Reputational.

**Solution:** Staff are encouraged to read the UC Email Management brochure which outlines appropriate email conduct that should be adhered to as a staff member at UC.
Marketing material sent to an alumnus, opens up concern regarding information being stored in the cloud, and incorrect management of personal information

Sally is a UC alumnus currently living in London. Recently she received some UC marketing material. This material is unrelated to her current situation and she is not interested in it. Sally contacts the University to let them know that she does not wish to be contacted with this type of information again in the future. An administrator at the University thanks Sally and says that they will remove her information from the database so she will not receive emails again in the future.

Sally receives another round of marketing material, and this time she becomes quite disgruntled. At the next UC event she approaches the Vice-Chancellor and has a go at him about how frustrated she is that the University has not managed her personal information appropriately. The University investigates the matter further and finds other occurrences of Sally’s contact details being stored in various spreadsheets within the department.

It comes to light that a deeper issue exists. The information was actually collected about Sally when she signed up to another UC event during her time in London, and was stored in an external database in an event organiser’s personal OneDrive account in the cloud. Not only has this opened up Sally’s information to the risk of hacking, but it has also meant that it was not captured as part of any central UC system. Therefore, she had signed up and given her information believing it was for one purpose, however this information was then used for marketing to her later. She was also not aware of the fact that her personal information was stored in the cloud.

**Issue:** Personal information is open to privacy breaches and misuse by not being collected and stored appropriately, and not being used strictly for the purposes it was collected. This poses risk to reputation, and annoyance of those the University has the support of. Personal information is vulnerable to hacking or mis-use by being stored in a cloud based system outside of NZ’s jurisdiction.

**Risks:** Reputational, Financial, Legal.

**Solution:** Sally’s details are updated in all relevant UC databases. Staff and organisers are advised not to store personal information in non-UC controlled external databases/the cloud. Processes are put in place for similar scenarios in the future, and a tick-box is added to data collection sheets so that people can opt-in to receive further emails/communications.
Information Breach – email containing personal information sent to the wrong person

As part of Michael’s job, he regularly sends out personal information to students via email. These emails usually contain the name of the person, plus what courses they have studied, their grade information, and sometimes financial information. On Friday after a long week, Michael stayed late at work in order to complete some work before the weekend. He quickly typed in an email address and hit send, but he did not check it before he sent it. On Monday morning Michael discovers that the auto-complete address function in Outlook has led to the email going to a student with a similar name, but not the correct student. This inadvertent recipient now has personal information about another student. The recipient is threatening to go to the media over the privacy breach because they do not believe that it is right for people to be receiving others’ personal information.

**Issue:** A privacy breach has meant that personal information has been released to the wrong person, who is disgruntled about it and may take the issue to the media.

**Risks:** Legal, Reputational.

**Solution:** The people involved are called in to meet and the situation is explained. Steps are put in place to prevent this from happening again, and apologies are made to both the recipient and the individual whose privacy was breached. Michael learns from his mistake and reads the UC Email Management brochure and UC Privacy Policy for tips on how to manage emails which contain personal information. He also discusses some options with his manager for preventing him working long hours and becoming tired or complacent.
10. Planning a work stream or project?

Use the Privacy Impact Assessment Tool below

The following privacy impact assessment tool helps you to get things right when you are dealing with people's information at UC. Use it when you are making decisions about how a project might be set up, how you will run an event, how you will capture peoples information, or how you might write up privacy statements when personal information will be involved.

a. Working or planning to work with personal information?

Do you collect information about people? If so, you need to think about how you are handing that information. The image on the front of this brochure is a useful reminder of how you can manage privacy correctly in your day to day work or project.

- Purpose relates to everything you do with personal information.
- It is the University's responsibility to be careful with the information it holds about people.
- Collection should be fair.
- The use of that information should be justified.
- Information should be disposed of appropriately when no longer needed.
b. Privacy impact assessment tool

Write up a simple analysis using the tool on page 14. This written record will be called your “privacy impact assessment”. Refer back to it frequently, and revise it if your project changes.

There is no “right” way of writing a privacy impact assessment. For a small project a simple table or bullet-point notes are enough. For more complex projects, a guidance handbook is available at the link below to assist you in preparing your privacy impact assessment. Make your privacy impact assessment as detailed as it needs to be to help you make the right decisions.

You can view more information about privacy impact assessment here in this handbook:

11. Queries

If you have any queries first seek out the Privacy Network Member from your area to see if they are able to help you, if not contact the IRM team on records@canterbury.ac.nz or Anita Kerr on 93889 or anita.kerr@canterbury.ac.nz

12. References

- Privacy Act 1993 (www.legislation.govt.nz)
- The UC Privacy Policy (www.canterbury.ac.nz/ucpolicy)
- General Disposal Authority (GDA) (www.canterbury.ac.nz/irm/documents/GDA.pdf)
- UC Policy Library (www.canterbury.ac.nz/ucpolicy)
- Email Management Brochure (www.canterbury.ac.nz/ VCOF3004_Email_Management_A5_Brochure)
Information and Records Management (IRM):

E: records@canterbury.ac.nz

Tom Norcliffe, Information and Records Manager
T: +64 3 364 2987 ext 93193

Anita Kerr, Senior Information Officer
T: +64 3 364 2987 ext 93889

Bjorn Gruebner, Information and Records Administrator
T: +64 3 364 2987 ext 93193

University of Canterbury
Te Whare Wānanga o Waitaha
Private Bag 4800
Christchurch 8140
New Zealand

www.canterbury.ac.nz/irm