Privacy Breach Notification Form

To be completed and then emailed to the University Privacy Officer (registrar@otago.ac.nz), and copied to the Deputy Privacy Officer (policycompliance@otago.ac.nz)

Please provide information on the privacy breach as specified below. You must complete all of the sections in this form. Please note that the information provided in this form will be used for any required reporting to the Privacy Commissioner.

Please contact the Privacy Officer or the Deputy Privacy Officer if you have any questions.

Section A – Reporter Details

Name:

Position:

Department:

Section B – Details of Privacy Breach

Please identify the type of privacy breach

- ☐ unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, Personal Information
- ☐ an action that prevents the University from accessing Personal Information

Personal Information means information about an identifiable individual – i.e. any information which tells us something about a person. The information does not need to name someone specifically, as long as they are identifiable in other ways. This can include (but is not limited to) that person's:

- *name*
- *address*
- *photo*
- *opinion or view*
- *employment information*
- *health records*
- *financial information*

Timeline

- The date of the privacy breach:
- The date the breach was identified (if different):
- Is the problem that caused this privacy breach ongoing: ☐ Yes ☐ No

Details

Please describe what has happened in detail, including:

- How many people were affected by the privacy breach (if known – use approximate numbers if necessary)
- The type(s) of Personal Information involved
- How did the privacy breach occur, what caused the breach
- Where the Personal Information has gone (if known)
- Whether the privacy breach is based on error or malicious intent (if known)

Section C – Mitigation

Please provide information on actions taken to mitigate/respond to the privacy breach.
It must include or address all of the following:

Notification of affected people

- Whether the affected individual(s) have been notified, and if so, how has this been done
- The response of affected individual(s) to notification (if known)
- If you have not notified the affected individual(s), the reasons why
- If you are delaying notifying the affected individual(s), the reasons why and for how long
- If you are relying on giving public notice to notify the people affected, the reasons why

Other organisations

- Any other organisations affected by the privacy breach, with an explanation of how they were affected
- Any authorities that the privacy breach has been reported to
- Any organisations that have been contacted that might be able to provide support to the University or to people affected by the privacy breach (eg CERT, ID Care, Netsafe, or any other)

Security

- Any information about the status of the Personal Information contained in the privacy breach (e.g. has it been returned or do we have reason to believe it has been destroyed)
- Any security measures in place that protect the Personal Information from being accessed

Other actions

- Any further planned actions to address the privacy breach
- Any actions to prevent a further privacy breach of this nature

Section D – Harm Assessment

The following questions will help us determine if the privacy breach is likely to cause anyone serious harm.

Sensitivity of information

How sensitive is the Personal Information that is involved in the privacy breach?

- ☐ Not sensitive
- ☐ Not likely sensitive
- ☐ Likely sensitive
- ☐ Sensitive
- ☐ Don't know

Sensitive information is typically Personal Information about someone's health, unique identifiers (e.g. passport or driver's licence number), genetic or ethnic background, political or religious beliefs, sex life or sexual orientation. Financial information, union affiliation or criminal history may also be considered sensitive. The disclosure of a person's sensitive information may cause them serious harm.

Please note any further details about the sensitivity of the Personal Information that is involved in the privacy breach

Recipient of information

Who has obtained or may obtain the Personal Information? Select all that apply:

- ☐ **Someone likely to cause harm**
  (The recipient(s) are likely to misuse or disclose the Personal Information in a way that causes harm. Includes employee browsing, unauthorised sharing, unauthorised access, theft, hacking and malicious activity preventing access)
- ☐ **Someone unlikely to cause harm**
  (The recipient(s) are unlikely to misuse or disclose the Personal Information, or don't have the ability to)
- ☐ **Someone uncooperative**
  (The recipient(s) are intentionally uncooperative (e.g. they refuse to return the Personal Information to you that was sent to them by mistake)
- ☐ **Someone unknown**
  (You know the Personal Information has been obtained by a 3rd party but don't know who)
- ☐ **Don't know**
  (You are certain that no unauthorised 3rd parties have obtained the Personal Information)

Please specify the names or other details of those persons, if known, including anyone else who may be able to obtain this information.

Types of Harm

What types of harm may be caused to people affected by the breach? Tick all that apply.
For each type of harm you identify, please also rate the likely impact you think it will have on any affected persons.

If you are uncertain how serious the impact is likely to be on one or more affected persons, err on the side of caution and select "High" rather than "Low".

Low impact - You believe the potential impact on the affected persons is less likely to be serious (e.g. have less of an effect on their lives).

High impact - You believe the potential impact on the affected persons is more likely to be serious (e.g. have more of an effect on their lives).

☐ **Discriminatory harm** ☐ Low ☐ High
(A person experiences discrimination as a result of a privacy breach where they are treated or are perceived to be treated differently because of their ethnicity, gender, disability, age, religious belief, sexual orientation or other identifying characteristic)

☐ **Emotional harm** ☐ Low ☐ High
(A person experiences anxiety, embarrassment, depression or hurt feelings as a result of a privacy breach. The knowledge that their personal information has been breached may cause someone)

☐ **Employment harm** ☐ Low ☐ High
(A person's job prospects or career progression are damaged or at risk as a result of a privacy breach e.g. personal information about a worker is accidentally or purposefully shared with their co-workers, damaging their standing within their organisation)

☐ **Financial harm** ☐ Low ☐ High
(A person experiences financial loss or is unable to access their money as a result of a privacy breach e.g. if someone is unable to access their bank account or if the personal information involved in the breach used by a 3rd party to steal money)

☐ **Identity theft** ☐ Low ☐ High
(A person uses someone else's personal information to pretend to be them e.g. if personal information that is stolen is used to apply for a passport in someone else's name)

☐ **Loss of access to information** ☐ Low ☐ High
(A person is temporarily or permanently unable to access their personal information)

☐ **Loss of opportunity** ☐ Low ☐ High
(A person loses out on opportunities as a result of a privacy breach e.g. they are not able to bring a case before court because their information has been lost or deleted, or they miss out on a scholarship or award)

☐ **Physical harm** ☐ Low ☐ High
A person experiences or is at risk of physical harm as a result of a privacy breach e.g. if a physical address disclosed as a result of a privacy breach makes it into the hands of someone who wishes to cause physical harm to another)

☐ **Reputational harm** ☐ Low ☐ High
(A person experiences damage to their reputation within their community or receives negative publicity that damages their reputation, as a result of a privacy breach)

☐ Threats of harm ☐ Low ☐ High

(A person is threatened with harm, such as blackmail, extortion or physical violence as a result of a privacy breach)

☐ Other (please specify): ☐ Low ☐ High

☐ Don't know

☐ None

Please indicate if you think any of the following applies:

Is someone's physical safety in immediate danger?

☐ Yes ☐ No

You believe someone may be at immediate risk of physical harm as a result of a privacy breach (e.g. if sensitive information about a person is accidentally sent to a violent ex-partner).

Is someone's psychological safety at immediate risk?

☐ Yes ☐ No

You believe someone may experience severe emotional distress or psychological injury as a result of a privacy breach.

Is someone at immediate risk of serious financial harm?

☐ Yes ☐ No

You believe someone is at immediate risk of losing wealth, property or other monetary benefits (e.g. if a person's banking information or credit card details are leaked online)

Likelihood of harm

How likely is it that someone will be harmed because of this privacy breach?

You may not have, or yet have, enough information to say for sure whether harm is likely to occur. Make your best assessment based on the information you have. If you suspect harm may occur, or are unsure but the potential harm to a person could be serious, err on the side of caution and select "Likely".

☐ Unlikely
☐ Likely
☐ Harm has already occurred
☐ Don't know

Attempts to reduce harm

What steps have been taken to reduce the risk of harm or further harm from this breach? Select all that apply.

☐ The Personal Information was recovered and not accessed
☐ The device was wiped remotely and the Personal Information was not accessed
☐ The problem that caused the privacy breach has been fixed
☐ The recipient(s) of the Personal Information were contacted
☐ Other. please specify:
☐ No action has been taken

Security measures

Are there any security measures in place that protect the Personal Information from being accessed?

Examples of security measures that may protect the Personal Information involved in the privacy breach from being accessed include:

- *If the Personal Information was encrypted and the encryption key to unlock the information is secure;*
- *If an account is protected by multi-factor authentication i.e. to access the account, the user must provide two or more credentials in order to confirm their identity (e.g. a login username and password AND a code sent to their mobile phone);*
- *If a document is password-protected and the password is not also exposed in the privacy breach (e.g. an email attachment that can only be opened with a password).*

☐ Yes ☐ No ☐ Maybe ☐ Don't know

Please add any other comments you may have about the risk of harm from the breach

Please attach any relevant supporting documents (if available).

Signed:

Date:

Office Use Only

Is employment information involved? ☐ Yes ☐ No

Has HR been notified? ☐ Yes ☐ No

Privacy breach harm assessment:

☐ Unlikely to result in serious harm

☐ Likely to result in serious harm

Was the online Privacy Breach Self-Assessment completed? ☐ Yes ☐ No

Has the Privacy Commissioner been notified? ☐ Yes ☐ No

If yes, date of notification:

Notes:

Completed by: **Date:**