Privacy Act 2020: Guidance for Staff Sending Personal Information Offshore

The Policy on Access to, and use of, Personal Information lays out the University rules on the disclosure of personal information. This is tightly controlled, however there may be limited circumstances in which disclosure, including to overseas institutions or colleagues, is acceptable, for example: moderation and marking, supervision, the provision of references, or approved research collaboration.

This guide is intended to assist staff who are legitimately disclosing personal information offshore, to ensure they meet the requirements of the new *Information Privacy Principle 12*, which only allows offshore disclosure under certain conditions. The Privacy Act 2020 and IPP12 come into effect from 1 December 2020.

This guide is intended for disclosure directly by staff. It does not apply to University systems, which are being dealt with separately, nor to using offshore cloud providers or other agents to hold or process information on the University's behalf (this is not considered offshore disclosure under the Act and so IPP12 does not apply). Please note that the University remains responsible for ensuring that privacy of personal information held on its behalf is protected, and this should be taken into account when using cloud providers or entering into agency agreements.

The University's Privacy Officer and Deputy Privacy Officer are working with various University groups to build compliance into existing processes (e.g. research ethics applications and University IT systems).

1. Is the information being disclosed information about an identifiable individual?

Where information is properly anonymised, no further action is required. However, you need to be certain that the information could not be linked in some way – whether directly or indirectly – to an identifiable individual.

Sending properly anonymised information is recommended where possible.

Note: Information about an identifiable individual is any information which tells you 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*

2. Is the disclosure to an individual or entity located in a country with privacy laws which provide the same level of safeguard as NZ privacy laws?

Disclosure to the following countries may be treated the same as disclosure within New Zealand, and does not require any special action:

- Any country that is part of the European Union
- United Kingdom
- Japan
- Australia (except where this relates to employee data)
- Israel
- Argentina
- Canada (commercial organisations)
- Andorra
- Faroe Islands
- Guernsey
- Isle of Man
- Jersey
- Switzerland
- Uruguay

If information to be disclosed is about an identifiable individual or individuals, and to a country other than those listed in point 2 above, then either **consent** or **agreement** will need to be pursued.

CONSENT

Personal information can be disclosed overseas if the individual(s) concerned provide their consent, after being expressly informed that the country to which their information is being sent may not provide the same privacy safeguards as exist under New Zealand law.

Normally, agreement (see below) is recommended over, or alongside, consent, but there may be some situations where consent alone is appropriate and more straightforward. Some examples where consent might be recommended:

- Supervision of a graduate research candidate, particularly where this is ongoing at 1 December 2020. Confirmation could be sought from the candidate via email that they remain happy for their thesis information and associated personal information to be shared with their offshore supervisor, despite that person being in a country which may not have the same level of privacy safeguards as New Zealand.

- Request for a reference. If the reference is for a role in a country not listed under 2 above, confirmation could be sought from the person asking you to be a referee that they are happy for you to provide a reference to a person or institution in a country which may not have the same level of privacy safeguards as New Zealand.

The Privacy at Otago webpage has a template consent email and consent form that can be used or adapted for seeking and recording consent.

AGREEMENT

IPP12 allows for overseas disclosure if you believe on reasonable grounds that the person or institution you are disclosing personal information to is required to protect the information in a way that, overall, provides comparable safeguards to those in the NZ Privacy Act. For University purposes, it is recommended this covers:

- Only accessing and using the information for the purpose for which it is provided.
- Not disclosing the information to any further party.
- Ensuring the information is secure and protected against loss, unauthorised access, disclosure, modification or other misuse.
- Disposal of the information once it is no longer required to be kept.
- The ability for the individual whose personal information is disclosed to seek access to and/or correction of their personal information.
- A commitment to advise the University as soon as practicable if a privacy breach occurs.

The level of evidence required to support this will depend on the nature and context of the information sharing. In some cases, contractual agreements may already be in place which give assurance that the conditions above will be met.

Otherwise, to assist with confirming expectations of overseas partners and documenting agreement, three resources are available to staff on the Privacy at Otago website which should cover most situations:

- An email template for confirming agreement with University expectations – this is recommended for use only with trusted partners, where minimal personal information is shared and risk of privacy issues arising are low. For example, this may be appropriate to support an existing supervisory arrangement.

- A simple agreement that can be signed by the overseas partner – this is recommended for use where more extensive personal information is shared, including on an ongoing basis, but the overall risk is still assessed as relatively low. This agreement gives a greater level of assurance than an email exchange. For example, this may be appropriate for moderation of assessment with an existing partner (if assessment cannot be provided in an anonymised form).

- A contractual agreement between the University and the overseas partner – this is recommended for ongoing exchange of more sensitive personal information, and provides a more formalised agreement. For example, this is recommended to support ongoing exchange of personal information in relation to a new research project.

Documentation

It is recommended that any consent or agreement sought (as above) be documented and held with your records. This should be available just in case a privacy issue arises at a later time.

Further Advice

For further general advice please contact the University Privacy Officer (registrar@otago.ac.nz) or Deputy Privacy Officer (policycompliance@otago.ac.nz). For any requests relating to employment information, please also include the Director of Human Resources (kevin.seales@otago.ac.nz) in any correspondence.