Understanding Privacy Law: your obligations as an organisation

This fact sheet summarises the Ask LOIS webinar on this topic, presented Natalie Neumann, Lawyer, Justice Connect on 10 March 2016.
This webinar can be viewed for free at www.asklois.org.au/webinars/past-webinars.

This factsheet looks at:
- Privacy law basics
- How to legally collect, use, handle and store personal information
- Systems and checks to put in place
- Avoiding and responding to privacy breaches

Who is Justice Connect?

Justice Connect helps people facing disadvantage who are ineligible for legal aid and cannot afford a lawyer - and the community groups who support them - to access free legal assistance.

Not-for-profit law (NFP law)

NFP law is a Justice Connect program. It is a specialist legal service for not-for-profit community organisations, providing information, training, advice and pro bono referrals, in NSW and Victoria. Its contact details are at the foot of this factsheet. Its services include:

- Legal Information Hub - factsheets for NFPs www.nfplaw.org.au
- Legal training for community groups
- Law reform work aimed at reducing unnecessary NFP regulation
- Phone advice to answer quick legal questions (limited service to eligible organisations)
- Referral to a lawyer to assist with complex legal issues (limited service to eligible organisations)

Other Justice Connect programs

- **Self Representation Service** – training, assistance and referrals for those who find themselves unrepresented in Fair Work, bankruptcy and human rights matters in the Federal and Federal Circuit Courts in NSW, Victoria, Tasmania and ACT.
- **MOSAIC** (Migrant Outreach Services - Advice, Information and Community Education) - for recently settled migrants, asylum seekers and refugees in NSW.
- **Homeless Law** - for clients experiencing homelessness or at risk of homelessness, with various outreach sites and targeted programs helping women facing homelessness and prisoners in Victoria.
- **Seniors Law** - for older clients with a legal issue associated with ageing, including elder abuse, including a new program placing lawyers in the healthcare system in Victoria.

How is privacy regulated?

Jurisdiction	Legislation	Regulator
Commonwealth	*Privacy Act 1988* (Cth)	Office of the Australian Information Commissioner (OAIC)
NSW	*Privacy and Personal Information Act 1998* (NSW) *Health Records and Information Privacy Act 2002* (NSW)	Information and Privacy Commission NSW (IPC)

Your organisation **must** comply with the Privacy Act if:

- its annual turnover is more than $3 million (including not-for-profits)
- it is a health service (broadly defined)
- it operates a residential tenancy database
- it is providing services under a Commonwealth contract
- it has 'opted in' to be covered by the Privacy Act

The Privacy Act contains the Australian Privacy Principles (APPs). The APPs are legally binding. They apply to most Australian Government agencies and many private sector organisations, together called APP entities.

It is **best practice** for an organisation to comply with the APPs even if it is not legally required to do so.

The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including higher standards for sensitive information). The APPs are drafted to be technology neutral, so that they apply equally to paper-based and digital environments.

Australian Privacy Principles	
APP 1: open and transparent management of personal information	**APP 7:** direct marketing
APP 2: anonymity and pseudonymity	**APP 8:** cross-border disclosure of personal information
APP 3: collection of solicited personal information	**APP 9:** adoption, use or disclosure of government related identifiers
APP 4: dealing with unsolicited personal information	**APP 10:** quality of personal information
APP 5: notification of the collection of personal information	**APP 11:** security of personal information
APP 6: use or disclosure of personal information	**APP 12:** access to personal information
	APP 13: correction of personal information

The Information Commissioner has also released Guidelines about the APPs. They are not legally binding but they are useful to show how the Commissioner will interpret the APPs. Those guidelines can be found here: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

What kind of information is covered by the APPs?

"Personal information" is any information or opinion about an identified individual, or an individual who is **reasonably identifiable.**

It is not limited to "private" or "sensitive" data and includes name, signature, address, phone number, date of birth, email address as well as photographs.

"Sensitive information" includes health, religion, race, sexual orientation, membership of professional associations or unions and criminal record.

"**Health information**" is a specific type of personal information which may include details about physical or mental health, or disability.

How to legally collect, use, handle and store personal information

Collection of personal information (APP 3)

Consent is required when collecting *sensitive* personal information but it is **not required** for the collection of *non-sensitive* personal information.

In both cases the information collected must be reasonably necessary for your functions/activities and must be collected by fair and lawful means.

Disclosure of personal information (APP 6)

Generally, you can only use or disclose personal information for the **primary purpose** for which it was collected. Unless:

- the person consents
- disclosure is required by law or court
- disclosure is reasonably expected and related (or directly related)

Cross-border disclosure (APP 8)

Before an APP entity discloses personal information to an overseas recipient, the entity must take **reasonable steps** to ensure that the overseas recipient does not breach the APPs.

Security of personal information (APP 11)

An APP entity must take reasonable steps to protect personal information it holds.

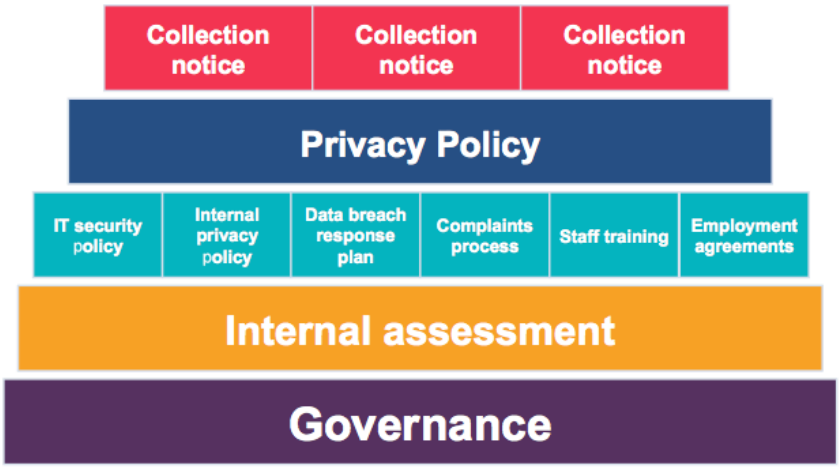
It must destroy or de-identify personal information once it is no longer needed (unless required by a law or court/ tribunal to retain the information).

NSW information sharing laws

Part 13A *Crimes (Domestic and Family Violence) Act 2007* deals with information sharing in cases of domestic violence:

- creates certain exceptions to NSW privacy laws
- does not create exceptions to Commonwealth privacy laws - service providers must comply with their obligations under the Privacy Act when they share information

Systems and checks to put in place



How do you ensure that you are complying with the privacy laws?

1. Governance systems in your organisation should be strong to ensure your organisation is aware of and complies with its legal obligations. Organisations should appoint a privacy officer to be responsible.
2. Do an internal assessment of your organisation. Look at the personal information you collect, how you collect it, consider the purpose of collecting the information so the individual can be informed.
3. The above image shows the types of policies you should have in place.
    I. A policy for IT security, including access to documents on staff's own devices.
    II. An internal privacy policy so staff know what they should be doing when handling personal information.
    III. A data breach response plan outlining the procedure in the event of a breach.
    IV. Complaints process if individuals wish to complain about a breach.
    V. Staff training session/s. Document details of the training to show to the OAIC in the event of a breach.
    VI. Employment agreements should include a note that staff understand they need to comply with the privacy laws.
4. APP entities must have a privacy policy in place, but it is a good idea even for organisations not bound by the APPs. The OAIC website has examples and checklists of what should be included https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-an-app-privacy-policy
5. Collection notices, mandatory for APP entities, are a useful tool for informing people what you plan to do with their information.

What to include in a collection notice (APP 5)

1. Name and contact details of entity collecting the personal information
2. Purpose for collection
3. Main consequences if the personal information is not collected
4. Who else the personal information may be disclosed to
5. Whether the personal information is likely to be disclosed to overseas recipients and if practicable, in which countries
6. Refer to Privacy Policy including: access, correction and complaints
7. If the collection is required or authorised by law or court/tribunal

Avoiding and responding to privacy breaches

Privacy breaches can occur as a result of **human error**, such as disclosing something without consent, or sending information to the wrong person by mistake.

Breaches also occur as a result of **technology failure**, such as when systems are hacked. Organisations must take reasonable steps to protect data from such attacks or failures.

There are four key steps in responding to data breaches:

1. Contain the breach and do a preliminary assessment
2. Evaluate the risks associated with the breach
3. Notification
4. Prevent further breaches

Notification of data breaches

There is currently no obligation to report data breaches **other than of health records**. However the OAIC encourages that entities do so voluntarily.

The *Privacy Amendments (Notification of Serious Data Breaches) Bill 2015* is currently before Parliament. If it passes, it will require mandatory notification of serious breaches

Complaints

An individual may complain to the OAIC if they consider that their privacy has been interfered with. The privacy commissioner can also investigate without a complaint but this is not common. Once a breach occurs, an individual has one year to make a complaint.

An individual will generally need to first lodge a complaint with the organisation itself. If a complaint is made to your organisation, it is probably best to deal with it before the complaint goes to the regulator. If there was a problem, consider admitting and offering some compensation.

Remember:

1. **Think about privacy at the outset**
2. **Think about trust and reputation of your organisation**
3. **Think about what people would reasonably expect of your organisation**
4. **Review and update your privacy policy**
5. **Have and use a collection notice**

Resources

- Not-for-profit Law Information Hub www.nfplaw.org.au/privacy
- Office of the Australian Information Commissioner www.oaic.gov.au
- Information and privacy commission NSW www.ipc.nsw.gov.au

Not-for-profit Law (NFP Law)
Website: www.justiceconnect.org.au/nfplaw
Phone: 1800 NFP LAW