LSC LEGAL SERVICES COUNCIL | COMMISSIONER FOR UNIFORM LEGAL SERVICES REGULATION

Privacy Management Plan

31 January 2021

LEGAL PROFESSION Uniform Law

Contents

Purpose

The *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA) requires that "each public sector agency must prepare and implement a privacy management plan within 12 months of the commencement of this section" (s 33). This plan explains how we manage personal information in line with PPIPA and health information under the *Health Records and Information Privacy Act 2002* (NSW) (HRIPA).

Further information about the PPIPA and the HRIPA are at Attachment A.

Who we are

The Legal Services Council (LSC) and Commissioner for Uniform Legal Services Regulation (Commissioner) were created by the Legal Profession Uniform Law (Uniform Law) which applies in NSW by virtue of the *Legal Profession Uniform Law Application Act 2014* (NSW) (NSW Application Act).

The Uniform Law commenced operation in NSW and Victoria on 1 July 2015. The Uniform Law applies in Victoria and NSW, in Victoria by virtue of the *Legal Profession Uniform Law Application Act 2014* (Vic).

The LSC's secretariat has six members of staff, including the Commissioner. The LSC comprises a Chair and five part-time members.

The LSC and Commissioner are subject to the PPIPA by virtue of the section 416 of the Uniform Law and section 6(1)(2) of the NSW Application Act, as modified by clause 5(1)(a) of the Legal Profession Uniform Regulations 2015 (Uniform Law Regulations). The LSC and Commissioner are not public sector agencies. However, clause 5(1)(a) provides that the LSC and Commissioner "are taken to be public sector agencies" for the purposes of the PPIPA. Although there is no reference to the application of the HRIPA to the LSC or Commissioner in the Uniform Law, NSW Application Act or Uniform Law Regulations, for convenience we have proceeded on the basis that these bodies are classified as public sector agencies for the purposes of the HRIPA.

For the above reasons, it is necessary that the LSC and Commissioner prepare and implement a Privacy Management Plan.

Under clause 17 of Schedule 1 to the Uniform Law the Chief Executive Officer (CEO) of the LSC is to administer the affairs of the LSC in accordance with the policies and directions of the LSC. The functions of the CEO are exercised by the Commissioner.

From time to time the LSC members may be provided with personal information in the course of their deliberations but this will very much be secondary to the legal, policy or management issue which the LSC may be considering.

However, as LSC members are also subject to the PPIPA, this manual and plan will be provided to LSC members to be formally noted by them. In future, when other members are appointed to the LSC, they too will be advised of the requirements of the PPIPA and HRIPA and will be expected and assisted by the Secretariat to comply with the PPIPA and Information Protection Principles (IPPs) and HRIPA and Health Privacy Principles (HPPs).

Nature of the LSC and Commissioner as organisations

The functions of the LSC and Commissioner are set out in the Uniform Law. In broad terms, they are required to oversee the implementation of the Uniform Law and to encourage other jurisdictions to join the Uniform Law scheme. The work that staff are required to undertake is in the nature of legal policy and advisory work and it requires high levels of accuracy, skill and experience.

Policies and practices to ensure compliance with the PPIPA and HRIPA

Section 20 of the PPIPA makes clear that the IPPs set out in the PPIPA apply to public sector agencies. As noted above, the LSC and Commissioner are subject to the PPIPA, effectively to equate them with public sector agencies. This means we proceed on the basis that the LSC and Commissioner are subject to the HRIPA as public sector agencies.

Because the LSC and the Commissioner are subject to the PPIPA and HRIPA this means that the Commissioner and all staff made available to the LSC by the NSW Department of Communities and Justice (DCJ) are also subject to the PPIPA and HRIPA. It is the policy of the LSC and Commissioner that staff must read and remain familiar with the IPPs set out in sections 8-21 of the PPIPA and the HPPs set out in Schedule 1 to the HRIPA.

Staff are instructed to comply with the PPIPA and HRIPA and are required to sign the instrument set out on the last page of this Plan to indicate that they are familiar with the IPPs and HPPs and the date on when they reviewed them. New staff must also familiarise themselves with this Plan, the PPIPA, the IPPs, the HRIPA and the HPPs as part of their induction. Staff are also required to be trained so that if they are unsure what to do about a privacy issue, they should approach the CEO or the Privacy Contact Officer.

The LSC devises its policies and practices by reference to the relevant provisions of the PPIPA and HRIPA and also by reference to the instructional information published by the Privacy Commissioner, including the “Guide to making Privacy Management Plans” and the Privacy Management Plan “Checklist”. Aside from the policies and procedures set out in this document, there are no other policies and procedures relevant to the Plan.

Compliance with IPPs and HPPs
Broadly, the IPPs and HPPs cover the collection, retention and security, access, alteration and checking of personal and health information. The IPPs and HPPs also place limits on use and disclosure of personal and health information.

Practices for compliance with the PPIPA and HRIPA
Most of the information held by the LSC and Commissioner is not personal or health information. It is more accurately described as legal or policy information. Personal information collected, retained, altered and disclosed is incidental to the performance of the policy and oversight functions of these entities. Health information collected relates only to employment matters of staff and could include medical certificates for sick leave or employee workers compensation matters (if any).

Neither the LSC nor the Commissioner directly regulate law practices, solicitors or barristers and do not have a complaint handling function. It shares the responsibility for regulation with the Legal Services Commissioners in Victoria and NSW and the professional bodies, which operate locally. However, both the LSC and Commissioner occasionally receive, in error, details of complaints about law practices, solicitors or barristers. When this occurs, the correspondence is forwarded to the correct regulatory body and the complainant is informed

that the correspondence has been forwarded to the appropriate authority in accordance with section 414 of the Uniform Law.

How we collect, store, use and disclose personal and/or health information

Collection

Information must only be collected by lawful means for purposes related to the functions and activities of the LSC or Commissioner.

Personal and/or health information collected and held by the LSC and Commissioner falls into four categories:

1. The personal and health information relating to LSC members, employees and student interns (if any).
2. Master lists of contact details for key stakeholders, including individuals.
3. Personal details disclosed to the LSC or Commissioner as part of a submission or through participating in other forms of consultation.
4. Documents lodged in error with the LSC or Commissioner relating to a complaint against a law practice, solicitor or barrister.

The details of these categories are:

1. The personal and health information of LSC members, employees and student interns is limited to that information which is relevant to the individual's position in the organisation. It is collected and retained for those purposes only and is to be retained for as long as it is relevant. This information is retained in the LSC electronic filing system.

2. The LSC also maintains a master contact list of names and addresses and other contact details. The list of names and addresses of Uniform Law stakeholders is kept up to date.

3. The LSC undertakes public consultation as part of the development of the Uniform Law and Rules and related policies, guidelines and directions. Personal information disclosed to the LSC, in the course of these processes, is collected for the purpose of the current consultation process and may be used for the purpose of future consultation and incorporated into the master contact list. The LSC also acknowledges each submission and requests consent before the submission is published. Personal information disclosed on a published submission is limited to the name of the author and the organisation. The person's address, email, phone number and signature are removed prior to publication.

4. When documents, letters or communications are lodged in error and are not solicited by the LSC or Commissioner, these are redirected to the correct regulatory authority and the sender is advised of this course of action. An electronic copy of the correspondence is kept in a secure folder as a record.

The LSC and Commissioner ensure that the personal and health information collected by them is relevant, accurate, not excessive and does not unreasonably intrude into the personal affairs of people. The information contains no more detail than has been provided and does not contain any other information.

The LSC will notify the individual that his/her personal or health information is being collected at the time of first request by the LSC. This notification will usually occur by email and, where reasonable, they will also be notified of matters such as the purposes for which the information is collected, the

intended recipients of the information and the existence of any right of access to, or correction of, the information. Where it is lawful and practical, we give people the option of remaining anonymous if preferred when providing personal or health information to us.

Generally, the LSC and the Commissioner do not collect sensitive personal information such as racial origin or sexuality.

Storage
The majority of information held by the Secretariat of the LSC and the Commissioner is contained on a computer shared drive. All electronic information is held on secured servers provided and maintained by the DCJ. Where information is stored in an electronic database, we ensure that appropriate descriptions are used. Sensitive information is held in a restricted access folder and particular care is exercised when dealing with it to ensure compliance with the IPPs.

Hard copy files are kept in offices that can only be accessed by staff with appropriate security access. The LSC and Commissioner dispose of hard copy information by way of shredding and electronic information in accordance with DCJ practices.

Use
It is the responsibility of all staff to ensure that use and disclosure of personal or health information is made in accordance with IPPs 10 and 11 (and, where applicable, HRPs 10 and 11). This includes only using the information for the purposes for which it was collected unless informed consent has been provided or an exemption to one of the IPPs or HRPs is met. Staff should not disclose the information to any person other than the person to whom information relates, unless one of the exceptions is met.

Disclosure
The LSC and Commissioner are subject to a general statutory prohibition on disclosure of any information obtained in the administration of the Uniform Law (section 462), unless a specified exemption applies (section 462(2)).

Contact information must be kept up-to-date and accurate to guard against accidental disclosure of personal information by sending a communication to the wrong person. Particular care must be taken when using electronic forms of communication, for example, when sending an email to multiple recipients, that the personal information of the other recipients is not incorrectly disclosed to any individual recipient. We also ensure that personal information is accurate before using it including by checking contact details directly with a person or their organisation.

Staff are required to update their personal and health information using the human resource application (SAP) as relevant. The onus is to keep their personal information up to date and accurate rests with the individual employee.

Dissemination of policies and practices within and outside the agency

Legal Services Council website
This Privacy Management Plan and the personal information collection notice (Attachment B) is included on the LSC website.

The “publications” tab on the LSC website indicates how publications can be accessed and provides a contact address where relevant documents are not published on the website. The publication guide refers to, for example, the Annual Report and LSC Guidelines, Directions and Information Sheets.

Exemptions
There are exemptions in the PPIPA and HRIPA that explain when an agency need not comply with the IPPs and HPPs. To date neither the LSC nor Commissioner has relied on any of these exemptions nor has any public interest direction been made in its favour by the Privacy Commissioner. Any change will be published by the LSC and/or Commissioner.

Public registers
The LSC has a simple online register of legal practitioners in Uniform Law jurisdictions, called the Australian Legal Profession Register. The register contains the name, type of practising certificate (solicitor or barrister only) and state where the practising certificate was obtained. This information is already publicly available on the websites of the designated legal regulatory authorities in participating jurisdictions. It does not contain reference to any personal information such as address, email or phone number. Users are directed to the relevant regulatory body to obtain further information about a legal practitioner, including accessing Registers of Disciplinary Actions.

Procedures for access, amendment, internal and external review

Access and amendment
A person wanting to access or amend their own personal or health information can make an informal request to the LSC or Commissioner. Generally, this request does not need to be made in writing. If a person is unhappy with the outcome of their informal request, they can make a formal application.

A person can make a formal application for access to personal or health information under the PPIPA or the HRIPA by writing to the LSC or Commissioner at LSC@legalservicescouncil.org.au.

The LSC or Commissioner will aim to respond to the formal application within 20 working days. They will contact the applicant to advise how long the request is likely to take, particularly if it may take longer than expected.

Privacy complaints
A person who is aggrieved by the way in which the LSC or Commissioner has handled their personal or health information may either make a complaint to the Privacy Commissioner or apply to the LSC or Commissioner for an internal review of that conduct. If a person considers the LSC or Commissioner has breached the PPIPA or the HRIPA the complaint can be resolved informally. Contact should be made with the LSC or Commissioner via e-mail, phone or in writing to raise the complaint.

If the applicant is dissatisfied with the outcome, a formal application for internal review may be lodged with the LSC or Commissioner.

Internal review process
If a person considers the LSC or Commissioner has breached the PPIPA or HRIPA relating to their person or health information, they may request an internal review under the provisions of the PPIPA.

Under section 53(3) of the PPIPA, an application for internal review must be lodged within six months from the date the applicant became aware of the conduct the subject of the application (however, the LSC or the Commissioner may consider a late application for internal review).

An internal review will be completed as soon as is reasonably practical or within 60 days from the date the application is received. An internal review will follow the process set out in the Office of the Privacy Commissioner's internal review checklist. When the internal review is complete, the LSC or Commissioner will notify the applicant in writing (within 14 days) of:

- the finding of the review
- the reasons for the finding, described in the terms of the IPPs and / or HPPs
- any action we propose to take
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal (NCAT).

The LSC or Commissioner will also send a copy of that letter to the Privacy Commissioner. Applicants are also able to lodge their complaint directly with the Privacy Commissioner.

External review
An application may also be made to the NCAT for an external review of the conduct that was the subject of a person's internal review application. However, a person must seek an internal review before they have the right to seek an external review.

Generally, a person has 28 days from completion of the internal review to seek an external review. The NCAT has the power to make binding decisions on an external review. For more information on how to request an external review please contact the NCAT.

Where a complaint is lodged pursuant to the HRIPA, the Privacy Commissioner may deal directly with the complaint.

Offences

Part 8 of the PPIPA and HRIPA contain offences for certain conduct of public sector officials and other persons including in relation to the following:

- corrupt disclosure and use of personal or health information by public sector officials
- offering to supply personal or health information that has been disclosed unlawfully
- offences relating to dealings with the Privacy Commissioner; and
- intimidation, threats or misrepresentation (HRIPA).

The LSC's strategies to minimise the risk of its employees committing an offence include obtaining a written acknowledgement by the employee that they have read this Privacy Management Plan and that they agree to comply with its requirements.

Related parties

The LSC has a service provider agreement in place with the DCJ for information technology and human resources systems and support. For this reason, personal or health information may be disclosed to the DCJ as part of this arrangement. The DCJ has its own Privacy Management Plan on its website.

Provision of Plan to Privacy Commissioner

Section 33(5) of the PPIPA requires agencies to provide a copy of the PIPPA Plan to the Privacy Commissioner as soon as practicable after it is prepared and whenever the Plan is amended. Accordingly, a copy of this Plan was provided to the Privacy Commissioner on 20 January 2020.

Data breach

If the LSC becomes aware of an information security breach, an investigation will be conducted and risk mitigation measures taken to prevent further breaches. Where appropriate the breach will be brought to the attention of the DCJ, as the host of the LSC's computer systems, and to the LSC.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (NSW) establishes a Notifiable Data Breaches (NDB) scheme. The NDB scheme applies to the DCJ as a tax file number recipient (TFN) as the DCJ holds TFN for employment and other business related purposes. A TFN recipient is any person who is in possession or control of a record that contains TFN information. A data breach may occur where personal information held by the DCJ is lost or subject to unauthorised access or disclosure.

A data breach or allegation of a data breach (regardless of whether it is captured by the NDB scheme or not) relating to any agency within the DCJ must be promptly notified to the Office of the General Counsel of the DCJ at infoandprivacy@justice.nsw.gov.au and to the Digital Technology Services at security.incident@justice.nsw.gov.au. This is of particular relevance where IT equipment (DCJ issued phones, laptops, database etc.) has been compromised or lost.

The Office of the General Counsel will coordinate a response to deal with the incident/alleged breach. Responding to a data breach notification to the Office of the General Counsel may include targeted inquiries about the nature and extent of the breach, notification of affected individuals, notifying the Privacy Commissioner and facilitating remedial action.

Amendments and version control

Section 33(4) of the PPIPA provides that an agency may amend its Privacy Management Plan from time to time. To facilitate amendments and version control, practices including the date of each amendment of this Plan are noted at the back of the Plan. This Plan will be reviewed on an annual basis from the date of last review/version.

Contacts

Legal Services Council **Privacy Contact Officer**	Bridget Sordo **T**: (02) 9692 1302 **E:** lsc@legalservicescouncil.org.au **Address**: PO Box H326, Australia Square NSW 1215
Office of the Privacy Commissioner (OPC)	**T**: 1800 472 679 **E**: ipcinfo@ipc.nsw.gov.au **Address**: Level 17, 201 Elizabeth Street, Sydney 2000
NSW Civil and Administrative Tribunal (NCAT)	**T:** 1300 00 NCAT or 1300 006 228 National Relay Service for TTY Users: 13 36 77 **Address:** John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

Version schedule

Version	Date	Reason for amendment
V0.1	28/04/2016	Initial draft
V0.2	8/06/2016	Final draft
V0.3	2/08/2016	Final document
V0.4	30/01/2019	Amended due to office move
V0.5	08/05/2019	Amended to include ALPR
V0.6	12/09/2019	Amended as per Office of General Counsel DCJ advice
V0.7	20/01/2020	Amended as per Information and Privacy Commissioner advice
V0.8	31/01/2021	Amended formatting and editing

Attachment A: *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA) and *Health Records and Information Privacy Act 2002* (NSW) (HRIPA)

The requirements of PPIPA and the HRIPA as how the LSC and Commissioner (we) manage personal and health information is as follows:

The PPIPA and personal information

The PPIPA sets out how we must manage **personal** information.

About personal information
Personal information is defined in s 4 of the PPIPA and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, family life, gender identification, sexual preferences, financial information, fingerprints and photos.

There are some kinds of information that are not personal information, e.g. information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public sector official. Health information is generally excluded here as it is covered by the HRIPA.

Information protection principles (IPPs)
Part 2, Division 1 of the PPIPA contains 12 IPPs with which we must comply. Here is an overview of them as they apply to us.

Collection
1. We collect personal information only for a lawful purpose that is directly related to our functions and activities.
2. We collect personal information directly from the person concerned.
3. We inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to us.
4. We ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.

Storage
1. We store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure.

Access and accuracy
1. We are transparent about the personal information we store, why we use the information and about the right to access and amend it.
2. We allow people to access their own personal information without unreasonable delay or expense.
3. We allow people to update, correct or amend their personal information where necessary.
4. We make sure that personal information is relevant and accurate before using it.
5. We only use personal information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose.
6. We only disclose personal information with people's consent unless they were already informed of the disclosure when we collected the personal information.

7. We do not disclose sensitive personal information without consent, e.g. ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.

The HRIPA and health information

The HRIPA sets out how we must manage **health** information.

About health information
Health information is a more specific type of personal information and is defined in s 6 of the HRIPA. Health information can include information about a person's physical or mental health such as a psychological report, blood test or an X-ray, or even information about a person's medical appointment. It can also include some personal information that is collected to provide a health service, such as a name and contact number on a medical record.

Health privacy principles (HPPs)
Schedule 1 to the HRIPA contains 15 HPPs that we must comply with. Here is an overview of them as they apply to us.

Collection
1. We collect health information only for a lawful purpose that is directly related to our functions and activities.
2. We ensure that health information is relevant, accurate, is not excessive and does not unreasonably intrude into people's personal affairs.
3. We collect health information directly from the person concerned.
4. We inform people why their health information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their health information and any possible consequences if they decide not to give their health information to us.

Storage
5. We store health information securely, keep it no longer than necessary and destroy it appropriately. We protect health information from unauthorised access, use or disclosure.

Access and accuracy
6. We are transparent about the health information we store about people, why we use the information and about the right to access and amend it.
7. We allow people to access their own health information without unreasonable delay or expense.
8. We allow people to update, correct or amend their health information where necessary.
9. We make sure that health information is relevant and accurate before using it.

Use
10. We only use health information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose.
11. We only disclose health information with people's consent unless they were already informed of the disclosure when we collected the health information.

Identifiers and anonymity
12. We do not use unique identifiers for health information, as we do not need them to carry out our functions.
13. We allow people to stay anonymous where it is lawful and practical.

Transfers and linkage

14. We do not usually transfer health information outside of NSW.
15. We do not currently use a health records linkage system and do not anticipate using one in the future. However if we did, we would not use one without people's consent.

Attachment B: Personal Information Collection Notice

Personal Information Collection Notice
By responding you may be giving personal information (such as name, email address and/or telephone contact) to the Legal Services Council and Commissioner for Uniform Legal Services Regulation (**we**, **us**, or **our**).

Who we collect the personal information from
We generally collect your personal information directly from you or from publicly available sources. However, in some cases, we may receive your personal information from a third party and when it is relevant to our statutory responsibilities (for instance during the course of consultation).

For what purposes do we collect personal information
We collect your personal information to perform our functions under the *Legal Profession Uniform Law, Legal Profession Uniform Law Application Act* 2014 (NSW) and the *Legal Profession Uniform Law Application Act 2014* (Vic).

What are the types of bodies and persons to whom we usually disclose your personal information?
Your personal information may be provided to:

- Regulators and government entities (such as the Office of the Legal Services Commissioner); and
- Organisations that represent the legal profession such as the Law Council of Australia, the Australian Bar Association, State Law Societies and State Bar Associations.

You can access and correct your personal information
Our privacy policy contains information about how you can access your personal information and seek correction of such information; as well as our compliance with *Privacy and Personal Information Protection Act 1998* (NSW). Our privacy policy is accessible via a link appearing on our website at: www.legalservicescouncil.org.au.

How to contact us
Write to:

Legal Services Council and Commissioner for Uniform Legal Services Regulation
PO Box H326
Australia Square NSW 1215

Email: lsc@legalservicescouncil.org.au