B. Confidentiality & Privacy

Applies to: All individuals who provide, or assist in the provision of legal services by SKLS	Version: 1.0
Specific responsibility: Executive Officer & Principal Lawyer	Date approved: 18 March 2019
	Next review date: 18 March 2020
Policy context:	
Standards or other external requirements	RM Guide NACLC National Professional Indemnity Insurance (**PII**) Scheme National Accreditation Scheme for Community Legal Centres
Legislation or other requirements	The Uniform Rules
Contractual obligations	National Partnership Agreement on Legal Assistance Services 2015-2020

1. INTRODUCTION

1.1 Unless stated otherwise, "**worker**" means employees and/or volunteers, as appropriate.

2. POLICY STATEMENT

2.1 SKLS recognises the importance of, and is committed to protecting and upholding, the privacy and rights of individuals SKLS deals with in relation to their personal information.

2.2 SKLS will ensure that:

(a) all information received from clients remains confidential and, other than as permitted under this policy, will not be discussed with third parties without consent;

(b) the identity of a client of SKLS or details regarding their legal problem will not be disclosed other than in accordance with this policy, unless consent has been given to do so;

(c) it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients, personnel and others;

(d) clients are provided with information about their rights regarding privacy;

(e) clients, personnel and others are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature; and

(f) all personnel understand what is required in meeting these obligations.

2.3 This policy explains how SKLS collects, uses, discloses and otherwise handles personal information. This policy does not apply to personnel records, however, it still applies to personal information about job applicants, contractors and volunteers or employees of related entities.

2.4 This policy will be addressed in staff, Board and volunteer orientation and training. All personnel are expected to comply with this policy and procedures contained within.

3. WHAT IS PERSONAL INFORMATION?

3.1 Personal information in general terms means any information that can be used to personally identify someone. It includes information or an opinion, whether true or not and whether recorded in a material form or not, about an individual who is identified or reasonably identifiable by the information.

4. WHAT IS SENSITIVE INFORMATION?

4.1 Sensitive information is a subset of personal information and is given a higher level of protection. Sensitive information is defined in the Privacy Act and includes information or an opinion about an individual's:

(a) racial or ethnic origin;

(b) political opinions;

(c) membership of a political association;

(d) religious beliefs or affiliations;

(e) philosophical beliefs;

(f) membership of a professional or trade association;

(g) membership of a trade union;

(h) sexual preferences or practices; or

(i) criminal record.

4.2 Sensitive information will only be collected with consent, unless special circumstances apply.

5. WHAT DOES PERSONAL INFORMATION DOES SKLS COLLECT AND HOW DOES SKLS COLLECT AND HOLD IT?

5.1 The type of information collected will depend on the nature of a person's interaction with SKLS, however, SLKS may collect the following types of personal information:

(a) identification and contact details, such as name, mailing or street address, email address, telephone number, age or birth date;

(b) family type, country of birth, year of arrival in Australia and language spoken at home;

(c) financial information, such as housing, occupation, financial status and income;

(d) sensitive information, such as racial or ethnic background, criminal history and health information, English proficiency, need for an interpreter, or disability;

(e) other personal or sensitive information not covered above which is collected as a result of providing a client with legal advice;

(f) details of the services a client has requested or enquired about, or services provided, together with any additional information necessary to respond or deliver those services; and

(g) any additional information relating to a client that a client provides.

5.2 SKLS collects personal information directly from an individual unless it is unreasonable or impracticable to do so. This may occur in a range of ways including: in person; by letter, fax, email or telephone; on hard copy forms; through the website; from referring or third parties (with consent); and at events or forums.

5.3 As far as possible, personal information should be collected in private. Care should be taken when collecting information from people in a public area.

Medical information

5.4 Information regarding a client's health, medical treatment or HIV status should only be collected if it directly relates to their legal matter.

5.5 Unauthorised disclosure of a person's HIV status is unethical and unlawful. If, in the course of handling a matter, the client has been or is required to be tested for HIV or is infected with HIV or AIDS, the lawyer must take all reasonable steps to protect the privacy of that person. Unless the HIV status of a person is directly related to their legal matter, it should not be noted on their file.

5.6 When correspondence is entered into on behalf of a client regarding their HIV status, lawyers should request that incoming correspondence be marked 'Private and Confidential'. Likewise, any outgoing correspondence should be marked 'Private and Confidential'.

6. NOTIFICATION OF COLLECTION OF PERSONAL INFORMATION

6.1 At the time that personal information is collected, or as soon as practicable afterwards, personnel should take reasonable steps to ensure that the person from whom the information is collected is aware of:

(a) who is collecting the information;

(b) why the information is being collected;

(c) what it will be used for;

(d) how the person can get access to the information;

(e) who else usually has access to the information;

(f) what the main consequences, if any, are for the person if they do not provide the information; and

(g) who else the information might be given to.

7. WHAT HAPPENS IF SKLS CAN'T COLLECT PERSONAL INFORMATION?

7.1 SKLS will give clients the option of interacting anonymously with SKLS, where general information only is sought. For specific legal advice, however, this will not be possible.

8. FOR WHAT PURPOSES DOES SKLS COLLECT, HOLD, USE AND DISCLOSE PERSONAL INFORMATION?

8.1 SKLS collects, holds, uses and discloses personal information for the following purposes:

(a) to assess whether a prospective client is eligible for assistance;

(b) to provide legal services, referral or arrangement of non-legal assistance to clients/prospective clients;

(c) to answer enquiries and provide information or advice about SLKS services;

(d) to recruit staff, contractors and volunteers;

(e) for planning, quality control and for the creation of anonymous case studies;

(f) to update records;

(g) for use in monitoring and assessing SKLS services, including as part of peer review of service, and reporting to funding providers;

(h) to process and respond to any complaints; and

(i) to comply with any law, rule, regulation or lawful and binding determination.

8.2 SKLS may also collect, hold use and disclose personal information for other purposes explained at the time of collection or which are required or authorised by or under law for which the individual has provided their consent.

9. TO WHOM MAY SKLS DISCLOSE PERSONAL INFORMATION?

9.1 SKLS may disclose personal information to:

(a) personnel, contractors or service providers for the purposes of providing legal services, fulfilling requests by clients, and to otherwise provide services to individuals including IT systems administrators, couriers, data entry service providers, electronic network administrators, and professional advisors such as accountants, solicitors, barristers and consultants;

(b) any organisation for any authorised purpose with the individual's express consent; and

(c) other third parties where required by law.

9.2 Personnel must not communicate, publish, release or disclose any personal information provided to them or SKLS in the course of the work, which is likely to lead to the identification of a client or clients and/or identification of a client's legal problem, except:

(a) in the course of the delivery of legal services;

(b) with the informed consent of the client where the client has the legal capacity to give consent;

(c) with the consent of the client's Parent or Guardian or Attorney under a Power of Attorney; or

(d) as required by law.

9.3 SKLS does not direct market, or provide personal information to other organisations for the purposes of direct marketing.

9.4 SKLS does not disclose personal information to anyone outside Australia.

9.5 All details that may identify particular individuals will be removed prior to statistical information being provided to meet the accountability requirements of funding bodies and others.

9.6 SKLS will not assign or adopt from another organisation unique identifiers (e.g. Medicare number or driver's licence numbers). SKLS will not disclose or use a unique identifier without consent except as required by law or as necessary in the provision of legal services.

10. ACCESSING AND CORRECTING PERSONAL INFORMATION

10.1 An individual may request access to any personal information SKLS holds about them at any time by contacting SKLS (see the details below). Where SKLS holds information that an individual is entitled to access, SKLS will try to provide the information in the manner requested (for example, photocopies or by viewing a file) and in a timely way. The Casework Lawyer must view the file and approve any copies of material to be given to the client prior to allowing the client access or copies.

10.2 There may be instances where SKLS cannot grant access to the personal information held. For example, SKLS may need to refuse access if granting access would interfere with the privacy of others or if it would result in a breach of confidentiality. However, there may also be other legal, professional or ethical duties that SKLS believes restricts the client's ability to fully access their file or prevents SKLS from allowing the client complete access to their file. If this occurs, SKLS will provide written notice outlining the reasons for the decision and available complaint mechanisms.

10.3 All requests for access to client files must be approved by the Principal Lawyer.

10.4 Professional reports are not accessible to the client if a restriction is requested by the author and the report has been requested by SKLS personnel.

10.5 SKLS takes reasonable steps to ensure that personal information SKLS collects, uses and discloses is accurate, up-to-date, and complete. Information that is not accurate, up-to-date or complete must be corrected as soon as possible upon SKLS becoming aware of this. The personnel who identifies inaccurate information is responsible for correcting the information or for making arrangements for it to be corrected.

Process to be followed if correction of information requested

10.6 If an individual believes that personal information SKLS holds about them is incorrect, incomplete or inaccurate, then they may request SKLS to amend it.

10.7 SKLS will then consider if the information requires amendment.

10.8 If SKLS agrees that it requires amendment SKLS will take reasonable steps to correct that information.

10.9 If SKLS does not agree that there are grounds for amendment then the individual may request that SKLS add a note to the personal information stating that the relevant individual disagrees with the information and SKLS will take reasonable steps to do so.

10.10 If SKLS corrects personal information about an individual and has previously disclosed that information to another agency or organisation that is subject to the Privacy Act, the individual may ask SKLS to notify that other entity and SKLS will take reasonable steps to do so, unless this would be impracticable or unlawful.

11. SECURITY AND INTEGRITY OF PERSONAL INFORMATION

11.1 SKLS takes reasonable steps to ensure personal information is protected from misuse and loss and from unauthorised access, modification or disclosure, including the following:

11.2 Only authorised personnel are to access client files and should only do so for authorised purposes.

11.3 Client files must not be left open on desks in central work areas. Files must remain closed, and preferably kept securely in filing cabinets when not in use. Filing cabinets should be kept closed when not in use, and locked when not in use for extended periods.

11.4 Client files may only be taken off the premises in very limited circumstances and for the briefest possible time. See SKLS *File Movement Policy* for further information.

11.5 Client information stored on computers should be password protected. Documents relating to clients should not be left unattended on the computer screen when not in use.

11.6 Care should be taken when discussing confidential or personal matters either in person or over the telephone.

11.7 When telephoning a client to confirm an appointment or for other reasons, if it is not possible to speak to the client directly, personnel should not identify themselves as being from SKLS. Personnel should use a first name, say that they are a friend or from St Kilda Community Centre and call back later on. The client may be seeking legal advice about a matter that concerns someone else who lives in the same place, for example, family violence, or may not wish other people to know about the issue.

11.8 For the same reasons, it is important that the client be asked about the most appropriate ways to contact them should the need arise.

12. DESTRUCTION OF PERSONAL INFORMATION

12.1 SKLS will take steps to destroy or de-identify personal information once it is no longer needed, in accordance with the SKLS Information Management Policy.

12.2 Files or documents that contain personal information are disposed of in a secure way. It is the responsibility of the Office Manager to ensure the secure disposal of personal information.

12.3 Client files will be closed once the legal matter is completed. Closed files and advice cards will be archived for specified periods as required by law.

13. COMPLAINTS

13.1 If an individual believes that their confidentiality or privacy has been breached, complaints may be made through the SKLS complaints procedures.