

<b>Policy Name</b>	<b>Privacy Policy</b>
<b>Date Last Reviewed</b>	February 2023
<b>Scheduled Review Date</b>	February 2024
<b>Approved By</b>	Board of Directors

### Purpose

The purpose of this Policy is to explain how Skyline Education Foundation Australia manages personal information that is provided to, or collected by, us.

If you need help to understand this Policy and you don't speak English, please contact us at [info@skylinefoundation.org.au](mailto:info@skylinefoundation.org.au) or call 0403 436 474.

A copy of this **Privacy Policy** is publicly available at [www.skylinefoundation.org.au/childsafety](http://www.skylinefoundation.org.au/childsafety). You can also request a copy by emailing [info@skylinefoundation.org.au](mailto:info@skylinefoundation.org.au). Before starting work, all Skyline staff, volunteers, contractors, service providers who work with children, and Board members are given a copy of this Policy.

Skyline is committed to protecting personal information in accordance with the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988 (Cth)*. When collecting and handling an individual's health information in Victoria, Skyline is also bound by the Health Privacy Principles (HPPs) set out in the *Health Records Act 2001 (Vic)*. In line with Victorian Child Safe Standard 7, Skyline ensures that our privacy law obligations are met as part of our child-focused complaints and concerns processes.

This **Privacy Policy** outlines the ways in which personal information, including sensitive information and health information, is collected, used, disclosed, stored, and secured. It also explains how you can access your personal information.

### Scope

This Privacy Policy applies to all individuals and entities that interact with Skyline Education Foundation Australia, including but not limited to:

- Staff
- Students, parents, carers, and families
- Board of Directors and Committee members
- Visitors, volunteers, contractors, and service providers
- Partners, donors, and other stakeholders.

The Policy covers the management of personal information, including sensitive and health information, that is collected, used, disclosed, stored, and secured by Skyline in the course of its operations, whether collected through solicited or unsolicited means. It also applies to any health information handled by Skyline under the *Health Records Act 2001 (Vic)*. This Policy governs the handling of all personal information under Skyline's control.

## Policy

### Collection of Personal Information

Skyline recognises that certain information provided by individuals may be considered private or personal. However, without this information, Skyline would not be able to carry out its operations and provide services and benefits to students.

### Sensitive Information and Health Information

Skyline is required by law to seek consent from an individual, or from a parent or carer if the individual is a student, before collecting sensitive information and health information, unless an exception applies. Examples of health records that contain health information include hospital admission forms, medical histories, test results, medication lists, and sick leave certificates. Generally, this type of information has a higher level of privacy protection than other personal information.

### Personal Information (Other Than Sensitive Information and Health Information) Provided Directly to Skyline

Where reasonable and practical, Skyline collects personal information directly from the individual or from parents or carers of student individuals. Personal information includes a wide range of information or an opinion that can identify an individual. What is considered personal information can vary depending on whether a person can be identified or is reasonably identifiable in the circumstances. Examples of personal information cited by the Office of the Australian Information Commissioner (OAIC), the regulator of the Privacy Act 1988 (Cth), include an individual's name, signature, address, phone number, date of birth, photos, IP addresses, voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique), and location information from a mobile device (because it can reveal user activity patterns and habits).

Skyline generally collects personal information directly in the following ways:

- Via face-to-face meetings, telephone calls, and verbal and written communications, including by social media, email, or mail, and keeping records of these communications.
- From forms filled out by prospective and current students, parents and carers.
- From prospective and current partners, donors, contractors, and service providers.
- From prospective and current Board and Committee members, staff, visitors, and volunteers.
- Through activity logs, cookies, and other data obtained from tracking technologies on Skyline's website and interactive learning portals.

Generally, Skyline will seek consent from the individual in writing before collecting their sensitive information and health information. However, given the nature of Skyline's operations, we may also receive personal information by email, letters, notes, via our website, over the telephone, in face-to-face meetings, and through financial transactions.

If you provide Skyline with the personal information of others, such as other family members, doctors or emergency contacts, we encourage you to obtain their consent and inform them that you are

disclosing that information to Skyline and why, so that they can request access and correct that information if they wish. You should also refer them to this **Privacy Policy** for further details about such requests and how Skyline otherwise handles personal information it collects.

#### **Personal Information (Other Than Sensitive Information and Health Information) Provided by Others**

Skyline may also receive personal information about an individual from third parties, e.g. where we use a third party provider to manage event registrations or conduct surveys, where we receive a report from a medical professional about an individual, or where we receive academic data or employment references.

We may collect information based on how individuals use our website. We use 'cookies' and other tracking technologies to collect information on website activity, such as the number of visitors, the number of pages viewed, and any internet advertisements which bring visitors to our website. This information is collected to analyse and improve our website, marketing campaigns, and to record statistics on web traffic. We do not use this information to personally identify individuals.

#### **Unsolicited Information**

Skyline may be provided with personal information without having sought it through our normal means of collection. This is known as 'unsolicited information' and is often collected by:

- a note from a student or their parents or carers
- misdirected postal mail – letters, notes, documents
- misdirected electronic mail – emails, electronic messages
- employment applications sent to us that are not in response to an advertised vacancy
- additional information provided to us which was not requested.

Unsolicited information obtained by Skyline will only be held, used and or disclosed if it is considered as personal information that could have been collected by normal means. If that unsolicited information could not have been collected by normal methods then we will destroy, permanently delete or de-identify the personal information as appropriate.

#### **Employee records**

Employee records are not covered by the APPs or the HPPs (except if the records contain health information). However, Skyline will use best efforts to ensure that the information is accurate, up to date, held securely within the organisation and disposed of in a secure manner.

#### **How Personal Information is Collected**

Skyline collects personal information in a number of ways, including:

- in person and over the phone from students, prospective students and their families, graduates, staff, volunteers, visitors, job applicants and others
- from electronic and paper documentation such as job applications, partner and donor applications, registrations of interest, emails, invoices, letters, and forms (such as enrolment, excursion, medical, specialist or consent forms)
- through our website and Skyline-controlled social media (e.g. Facebook)
- through online tools such as apps and other software used by Skyline
- via any CCTV security cameras located at Skyline premises



Education Foundation Australia

- through photographs, film and other recordings
- from polls, surveys and questionnaires
- in some cases, through authorised information sharing arrangements with other services.

### **Use of Personal Information**

Skyline only uses personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected by the individual, or for an activity or purpose to which an individual has consented. For example, personal information might be used to keep students and stakeholders informed about our ongoing activities, to assess applications for our programs and benefits, and to assist us in improving our services.

Skyline's primary uses of personal information include, but are not limited to:

- maintaining individual student or donor records and a comprehensive database to assist us in providing education, emotional and practical support to students, including through personal growth and development workshops, vocational seminars, a residential workshop, networking opportunities, and reimbursement of educational expenses
- providing information to students and others about how to access our services and benefits
- satisfying our legal obligations including duty of care, child safety, and wellbeing obligations
- keeping parents and carers informed about Skyline community matters through correspondence, newsletters, and magazines
- marketing, promotional, and fundraising activities
- supporting community-based causes and activities, charities, and other causes in connection with Skyline's functions or activities
- helping Skyline to improve its day-to-day operations, including training staff and volunteers
- systems development, developing new programs and services, and undertaking planning, research, and statistical analysis, including to identify and analyse the needs of Skyline students and their families, and to identify future potential students, services, and benefits
- administration, including for insurance purposes
- employing staff and engaging volunteers, contractors, and service providers.

Skyline will only use or disclose sensitive information or health information for a secondary purpose if an individual would reasonably expect us to use or disclose the information, and the secondary purpose is directly related to the primary purpose. Skyline may share personal information with related organisations, but only if necessary for us to provide our services and benefits.

Skyline will not use personal identification numbers that have been assigned to an individual by a government department or agency.

### **Disclosure of Personal Information**

Skyline uses personal information for the purposes for which it was provided, or for purposes that are directly related to our functions or activities. Personal information may be disclosed to various parties, including government agencies, schools, employees, service providers, contractors, and other recipients, if the individual has given consent or would reasonably expect the information to be disclosed in that manner.

Skyline may disclose personal information without consent or in a manner that an individual would reasonably expect if:

- We are required to do so by law, for example, to comply with subpoenas, warrants, or other court orders, or to report certain matters to an agency or enforcement body, such as suspected cases of child abuse
- The disclosure will lessen or prevent a serious threat to the life, health, or safety of an individual or to public safety
- Disclosure is reasonably necessary for a law enforcement-related activity (e.g., Australian Federal Police, Customs, Victoria Police, Australian Crime Commission, Immigration Department, ASIC, AUSTRAC, APRA)
- Another permitted general situation applies (e.g., taking action in relation to suspected unlawful activity or serious misconduct, locating a missing person)
- Another permitted health situation exists (e.g., conducting research, compiling or analysing statistics, disclosure to a person responsible for the individual, or to prevent a serious threat to the life, health, or safety of a genetic relative of the individual).

Skyline may disclose personal information to overseas organisations when providing our services, for example, when storing data with a "cloud service provider" located outside Australia. Skyline will take reasonable steps not to disclose an individual's personal information to overseas recipients unless we:

- Have the individual's consent (which consent may be implied)
- Are satisfied that the overseas recipient is compliant with the APPs, or a similar privacy regime.
- Form the opinion that the disclosure will lessen or prevent a serious threat to the life, health, or safety of an individual or to public safety
- Are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

### Storage and Security of Personal Information

Skyline stores personal information in various formats, including databases, hard copy files, personal devices, third-party storage providers such as cloud storage facilities, and paper-based files.

To ensure the privacy and security of this information, Skyline takes all reasonable steps to prevent its misuse, loss, unauthorised access, modification, or disclosure.

These steps include, but are not limited to:

- Restricting access to information and user privileges based on staff roles and responsibilities
- Ensuring staff do not share personal passwords
- Storing hard copy files in lockable filing cabinets in secure rooms, with access restricted to authorised personnel
- Securing access to Skyline premises at all times
- Implementing physical security measures around Skyline buildings and grounds to prevent unauthorised entry
- Maintaining IT and cybersecurity systems, policies, and procedures and ensuring they are up to date
- Requiring staff to comply with Skyline policies and procedures when handling information, including the **Record Keeping Policy and Procedures**
- Destroying, deleting, or de-identifying personal information that is no longer needed or required to be retained by law.

### Responding to Data Breaches

Skyline is committed to taking appropriate and prompt action if we have reasonable grounds to believe

**Commented [RG1]:** Should we be storing personal information on personal devices?

**Commented [RG2]:** Do we gain assurance from third-party storage providers around the security of their facilities?

that a data breach may have occurred or is suspected to have occurred. Depending on the nature and severity of the breach, we will conduct a review of our internal security procedures, take remedial action, and notify affected individuals and the Office of the Australian Information Commissioner (OAIC). If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to ensure the statement is brought to the attention of those affected.

#### **Website links**

Our website may contain links to other websites, and those third-party websites may collect personal information from individuals. Skyline is not responsible for the privacy practices of other businesses, or the content of websites linked to our website. We encourage users to be aware when leaving Skyline's website and to read the privacy statements of each and every website that collects identifiable personal information. It is important to note that these websites are not governed by this **Privacy Policy**.

#### **Student Personal Information**

The *Privacy Act 1988 (Cth)* applies to all individuals, regardless of their age, and does not set a minimum age for individuals to make decisions regarding their personal information. To comply with the *Privacy Act 1988 (Cth)*, Skyline may seek and obtain consent directly from students, particularly in situations where sensitive or health information is involved. We recognise that in some cases, a student may give or withhold consent independently from their parents or carers.

However, there may be circumstances where Skyline denies access to information to parents or carers if providing the information would have an unreasonable impact on the privacy of others or if it would result in a breach of our duty of care to the student.

We take a common-sense approach when handling a student's personal information, and in general, we will refer any requests for personal information to the student's parents or carers. Notices and consents provided by parents or carers are considered to be notices and consents provided by the student.

#### **Quality of Personal Information**

Skyline has implemented practices, procedures, and systems to ensure that the personal information we collect, use, disclose, and store is accurate, up-to-date, complete, and relevant at the time it is collected and used or disclosed. This also applies to health information.

#### **Accessing and Correcting Personal Information** (not including Health Information)

Individuals have the right to request access to their personal information held by Skyline. Upon receiving such a request, Skyline will take reasonable steps to verify the individual's identity before granting access or correcting the information.

Skyline will provide access to personal information where the request is in accordance with the APP, subject to limited exceptions. These exceptions include where the access would be unlawful, pose a serious threat to the life or health of another individual, unreasonably impact the privacy of others, or involve commercially sensitive or legally privileged information.

If an individual advises Skyline that their personal information is inaccurate, Skyline will take reasonable steps to correct the information once the individual's identity has been confirmed. To ensure confidentiality, details of personal information will only be provided where Skyline is satisfied the information relates to that individual.

Requests for access to personal information will be responded to within a reasonable time. If access is denied, Skyline will provide written reasons for the refusal (except where it would be unreasonable to do so) and information about how to make a complaint.

It's important to note that Skyline is not required to grant access to employee records under the *Privacy Act 1988 (Cth)* unless the information is used for a purpose not directly related to the employment relationship. However, access may be requested pursuant to workplace laws that require certain information to be made and kept for each employee.

### Accessing and Correcting Health Information

As outlined by the Victorian Health Complaints Commissioner, under the Health Privacy Principles (HPP), individuals have the right to access and correct any health information held about them. Skyline may, in some circumstances, refuse to provide access to health information or to correct it. If so, we must provide written reasons for the refusal.

Similar exceptions apply as stated above, including cases where:

- Skyline believes on reasonable grounds that providing access would pose a serious threat to the individual's life or health or the life or health of any other person
- the health information has been provided in confidence by a person other than the individual or another health service provider (such as a relative or friend) on the understanding that the information would not be revealed to them.
- providing access would, in Skyline's opinion:
  - have an unreasonable impact on the privacy of other people
  - reveal Skyline's intentions in relation to negotiations, other than about the provision of a health service, with the individual in such a way as to expose the organisation unreasonably to disadvantage
  - be unlawful
  - be likely to prejudice an investigation of possible unlawful activity
  - be likely to prejudice a law enforcement function by or on behalf of a law enforcement agency
- the information relates to existing legal proceedings between the individual and Skyline, and the information would not be accessible by the process of discovery in those proceedings or is subject to legal professional privilege
- denying access is required or authorised by law:
  - a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would likely damage Australia's security
  - the individual has already unsuccessfully made a request for the information at least once before, and there are no reasonable grounds for making the request again
  - the individual has already been provided with access to the health information and is making an unreasonable, repeated request for access to the same information in the same way.

Skyline will take reasonable steps to correct inaccurate health information upon receiving the individual's advice to this effect once their identity has been confirmed. Skyline may require the request to be made in writing and proof of identity. Requests made on behalf of another person must

be in writing and confirm evidence of their authority to act on the other person's behalf. If the information is considered correct, complete, and up to date, the individual can provide us with a written statement detailing the items they want corrected, and we will keep this statement with the records. To ensure confidentiality, details of health information will only be passed on where Skyline is satisfied the information relates to that individual.

Skyline will respond to a request for access to health information within a reasonable time. If access is denied, we will provide written reasons for the refusal (except where it would be unreasonable to do so) and the mechanisms available to complain about the refusal.

For more information, visit <https://hcc.vic.gov.au/public/health-records-individuals>.

### Complaints

If you have a privacy concern or complaint regarding the handling of your personal information by Skyline or any person within Skyline, we encourage you to raise the concern or complaint in accordance with our Complaints Policy. This policy provides easy-to-understand and accessible information on how to make a complaint and is publicly available on our website at [www.skylinefoundation.org.au/childsafety](http://www.skylinefoundation.org.au/childsafety).

If you are not satisfied with the outcome of your privacy concern or complaint related to your personal information, you have the right to request external review by the Office of the Australian Information Commissioner (OAIC). However, please note that the OAIC advises that it is unlikely to investigate a complaint about an organisation's mishandling of personal information unless a complaint is first made to the organisation. More information on how to make a privacy complaint to the OAIC, including that complaints must be in writing, is available on their website at <https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us>.

If you have a privacy concern or complaint related to the handling of your health information by Skyline, you can make an official complaint to the Health Complaints Commissioner. The Commissioner can investigate privacy breaches or incidents related to health information under the Health Records Act 2001 (Vic). More information on how to make a complaint about health information is available on their website at <https://hcc.vic.gov.au/providers/reporting-privacy-breaches-or-incidents-hcc>.

### Breach

Skyline staff, volunteers, contractors, and service providers who breach this **Privacy Policy** may face disciplinary procedures in accordance with their employment agreement, relevant industrial instrument, professional code, or terms of engagement.

The following actions may be taken, depending on the nature of the relationship and the severity of the breach:

- Remedial education
- Counselling
- Increased supervision
- Restriction of duties
- Appointment to an alternate role
- Suspension
- Termination of employment, contract, or engagement in the case of serious breaches.

These measures are not exhaustive and are subject to the discretion of Skyline management.



**Compliance monitoring**

Compliance with this Policy will be closely monitored by the CEO, who may conduct independent audits and reviews. Our aim is to ensure that the **Privacy Policy** is fully implemented and followed by everyone, including contractors and service providers who undertake child-related work. Our leaders are expected to champion and model compliance by taking a proactive, outspoken approach on the importance of child safety and wellbeing. They are expected to 'walk the talk' by taking child safety matters seriously, responding promptly and thoroughly to any concerns, and helping to embed child safety practices throughout Skyline.

**Review**

Skyline is committed to providing a safe and supportive environment for children, and we continuously work to improve our Child Safety Program. Ensuring compliance with privacy laws is a fundamental aspect of our efforts to promote positive, child-centered, and culturally safe procedures for handling complaints and concerns. To this end, we have established robust mechanisms for reviewing and enhancing our child safety policies, procedures, and practices, and for monitoring compliance with all relevant laws, regulations, and standards. Our processes include:

- Regular reviews of the Privacy Policy by the CEO, at least every two years, or after any significant child safety incident or breach of policy, and seeking feedback from staff, volunteers, students, families, and the wider Skyline community.
- Using best practices and engaging in stakeholder consultations to inform the development and revision of our policies and procedures, involving those relevant within Skyline.
- Capturing and analysing all complaints, concerns, and safety incidents to identify any underlying causes and systemic failures and to inform continuous improvement. Whenever we identify any shortcomings or deficiencies in our policies, procedures, or practices, we take swift actions to prevent them from reoccurring.
- Ensuring transparency by sharing reports on the findings of relevant reviews with all members of staff, volunteers, families, students, and the wider Skyline community.

Our commitment to continuous improvement means that we regularly review and update our Child Safety Program to ensure that it is effective, relevant, and responsive to the needs of our community. By doing so, we aim to provide a safe and inclusive environment that promotes the wellbeing and empowerment of all children who are part of Skyline.

**Definitions**

The following terms in this Privacy Policy have specific definitions (and are consistent with law where indicated):

Child	Child means a child or young person who is under the age of 18 years. <a href="#">Source: Child Wellbeing and Safety Act 2005 (Vic)</a>
Health information	In relation to Skyline (as an organisation that is not providing a health, disability or aged care service), 'health information' means information or an opinion about: (i) the physical, mental or psychological health (at any time) of an individual; or (ii) a disability (at any time) of an individual; or (iii) an individual's expressed wishes about the future provision of health services to him or her; or (iv) a health service provided, or to be provided, to an individual— that is also personal information.

**Commented [RG3]:** Suggest to footnote sources

	<p><b>NOTE:</b> personal information in this context is similarly defined as below, but additionally under the Health Records Act it does not include information about an individual who has been deceased for more than 30 years.</p> <p>Health information also includes personal information originally collected in the course of providing a health, disability or aged care service to an individual or collected in connection with the donation of human tissue and genetic information that is or could be predictive of the health of an individual or their descendants.</p> <p>Source: <i>Health Records Act 2001 (Vic)</i></p>
Individual	<p>Individual means a 'natural person' so does not include a body politic or corporate entity, including a company.</p> <p>Source: <i>Privacy Act 1988 (Cth)</i></p>
Personal information	<p>Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:</p> <p>(a) whether the information or opinion is true or not; and</p> <p>(b) whether the information or opinion is recorded in a material form or not.</p> <p>Source: <i>Privacy Act 1988 (Cth)</i></p>
Sensitive information	<p>Sensitive information means:</p> <p>(a) information or an opinion about an individual's:</p> <ul style="list-style-type: none"> <li>(i) racial or ethnic origin; or</li> <li>(ii) political opinions; or</li> <li>(iii) membership of a political association; or</li> <li>(iv) religious beliefs or affiliations; or</li> <li>(v) philosophical beliefs; or</li> <li>(vi) membership of a professional or trade association; or</li> <li>(vii) membership of a trade union; or</li> <li>(viii) sexual orientation or practices; or</li> <li>(ix) criminal record;</li> </ul> <p>that is also personal information; or</p> <p>(b) health information about an individual; or</p> <p>(c) genetic information about an individual that is not otherwise health info; or</p> <p>(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or</p> <p>(e) biometric templates.</p> <p>Source: <i>Privacy Act 1988 (Cth)</i></p>

#### Skyline policy and procedure linkages

- Child Safety and Wellbeing Policy
- Child Safety Code of Conduct
- Child Safety Responding and Reporting Obligations Policy and Procedures
- Complaints Policy and Procedures
- Record Keeping Policy and Procedures.

#### Related legislation

The following legislation, standards and regulations apply, and this Policy and Procedures align with these mandated requirements:

- *Child Wellbeing and Safety Act 2005 (Vic)* and the Child Safety Standards made pursuant to that Act
- *Health Records Act 2001 (Vic)*



Education Foundation Australia

- *Privacy Act 1988 (Cth)*.

#### **References and Resources**

In addition to the information referred to in this Policy, further information on the OAIC can be obtained via their website at <https://www.oaic.gov.au/>.

The OAIC also has references to, and guidance on, the APP including the Australian Privacy Principles quick reference, available at <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference>.