Privacy Policy - Workers

Sponsor: Sundale Board

Organisational Statement

Sundale takes its privacy obligations seriously and is committed to handling personal information in a transparent, lawful and secure manner consistent with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Aged Care Act 2024 (Cth), and other applicable legislation. Sundale is committed to privacy by design, responsible information handling practices, and maintaining appropriate technical and organisational measures to protect personal information. It is important that individuals understand and support Sundale's obligations and feel confident about reporting any actual or suspected breaches of privacy without fear of harm or reprisal.

Scope and application

This Privacy Policy (**Policy**) applies to everyone who works at Sundale, including employees and Board members, volunteers or unpaid work experience students, contractors, consultants, and labour hire workers who perform work for Sundale (collectively **workers**) whenever they are performing their duties or dealing with any personal information.

This Policy sets out:

(a) Sundale's obligations with respect to workers' personal information; and

(b) Sundale's expectations of all workers with respect to privacy.

Sundale has an appointed Privacy Officer who is responsible for implementation of this policy and all matters of privacy within Sundale. If there are any queries about this policy, or any issues which arise in respect of Sundale's dealings with personal information, please consult the Privacy Officer by email at privacy@sundale.org.au, or by phone on 1800 786 325.

Sundale's obligations to workers

General

Sundale is bound by the Applicable Laws, recognises the importance of privacy, and is committed to protecting the personal information collected from workers.

Sundale is required by the Fair Work (FW) Act to collect certain information about employees, including name, basis of employment, rate of pay, information about deductions and entitlements, superannuation fund details and information about Sundale payments into that fund, and information relating to an employee's termination. The requirement to collect this information will not apply to all workers, as not all workers are employees of Sundale.

Sundale will train all workers in appropriate privacy procedures in line with the Applicable Laws, including via making this Policy available to workers.

Collection

Types of information collected

Sundale may collect and hold personal information about a worker (that is, information that can identify the worker) relevant to employing or engaging the worker. This may include:

- names, contact details, and date of birth
- personal information contained within an application and CV / resume;
- employment history;
- personal information derived from a reference;
- personal information derived from an interview or otherwise during the engagement and onboarding process (including through any psychometric or other testing);
- bank account and superannuation fund information;
- tax file number;
- ABN;
- wage and entitlement information and other payroll information;

- personal and emergency contact information;
- licenses and other certificates and qualifications;
- information included in a passport, birth certificate, visa or other documentation demonstrating a worker's right to work in Australia;
- relevant medical information pertaining to employment or workplace injuries;
- information relating to a worker's performance or conduct;
- information relating to a worker's engagement, training, disciplining, and resignation / termination;
- the terms and conditions applicable to the worker; and
- photographs, videos, and other recordings.

Sundale may also collect and hold Sensitive Information about workers, if the worker consents to the collection of the information and if the information is reasonably necessary for the performance of Sundale's functions and activities. Where required by law, Sundale will obtain express consent before collecting sensitive information. In limited circumstances permitted by law, consent may be implied or may not be required.

Sundale may also collect information regarding a worker's use of Sundale systems, devices, applications and digital services, including access logs, system activity records, authentication records, security monitoring information and other information necessary to maintain information security, fraud prevention and business operations. Information collected through these processes will be managed in accordance with this Policy and applicable laws.

Method of collection

Sundale will generally collect personal information directly from workers through a variety of avenues, including any application process, use of Sundale's standard forms (such as onboarding forms), emails or other communication avenues, and in person.

There may, however, be some instances where personal information or health information about a worker will be collected indirectly because it is unreasonable or impractical to collect personal information directly from that worker. For example, Sundale may collect personal information from referees when they provided references, academic institutions or training and certification

providers, providers of license and background-checking services, recruiters and other service providers who assist in the engagement process, and other publicly available sources such as social media platforms. Sundale will usually notify workers about these instances in advance, or where that is not possible, as soon as reasonably practicable after the information has been collected.

If Sundale receives unsolicited information about a worker that it did not request and which is not directly related to Sundale's functions or activities (including its function as an employer or principal of a contract), Sundale may be required to destroy or de-identify that information, providing it is lawful and reasonable to do so.

We may also collect information through Sundale websites, employee portals, digital applications, communication platforms and other technology systems. This may include user preferences, device information, usage information, authentication information, cookie information, geographical location information and security monitoring data where reasonably necessary to support Sundale's operations, cyber security obligations and workforce management functions.

Purpose of collection

Generally, Sundale will collect, use and hold a worker's personal information if it is reasonably necessary for, or directly related to, the performance of Sundale's functions and activities, including facilitating Sundale's internal business operations, including maintaining and managing the employment or engagement of the worker, terminating the employment or engagement of the worker, the fulfilment of any legal requirements, and analysing Sundale's worker needs with a view to developing new or improved business operations.

Automated Decision-Making

Sundale may use computer programs, artificial intelligence systems, machine learning tools, workflow automation technologies and other automated processes to assist with workforce administration, recruitment, rostering, training allocation, fraud detection, cyber security monitoring, system access management, workforce analytics and other business functions.

Where personal information is used in an automated decision-making process that could reasonably be expected to significantly affect a worker's rights or interests, Sundale will describe:

- the kinds of personal information used by the automated process;
- the kinds of decisions made or materially assisted by the automated process; and
- any other information required by applicable privacy laws.

Sundale will maintain transparency regarding such practices through its privacy notices, Privacy Collection Statements and Privacy Policies. Sundale will maintain appropriate governance and human oversight of automated decision-making processes where required by law, policy or operational risk considerations.

The use of AI tools by workers must also comply with Sundale's Acceptable Use Policy, including requirements for approved tools, human validation and protection of personal, sensitive and classified information.

Failure to provide information

Depending upon the circumstances, a worker's refusal to provide personal information or consent to Sensitive Information being collected or held for the purposes set out in this Policy may adversely affect Sundale's ability to comply with its legal obligations and its ability to continue its relationship with the worker.

Use and disclosure

Generally, Sundale only uses or discloses personal information for the purposes for which it was collected (as set out above). Sundale may disclose personal information about a worker to:

(a) its employees, contractors, consultants, and other parties who require the information to assist Sundale with establishing, maintaining, managing, or terminating the relationship with the worker;

(b) Sundale's related entities to facilitate Sundale's and their internal business processes;

(c) third party service providers who assist Sundale in operating their business (including payroll and payment processors, insurers, superannuation funds, IT and technology

service providers, and professional advisers such as lawyers, accountants, and auditors);

(d) third parties to whom the worker has agreed Sundale may disclose the worker's information or where the information was collected from the worker for the purposes of passing it on to the third party; and

(e) any other entity as otherwise permitted or required by law.

Sundale may expand or reduce its business, and this may involve the sale and/or transfer of control of all or part of its business. Personal information, where it is relevant to any part of the business for sale and/or transfer, may be disclosed to a proposed new owner or newly controlling entity for their due diligence purposes, and upon completion of a sale or transfer, will be transferred to the new owner or newly controlling party to be used for the purposes for which it was provided under this Policy. Additionally, in circumstances of a business sale, Sundale is required under the FW Act to transfer employment records for each employee transferring to the new employer on request by the new employer.

Disclosure of personal information overseas

Sundale is assisted by a variety of external services providers to operate its business, some of whom may be located overseas. These third parties are too numerous to list, and they change from time to time. Some examples of the types of third parties include technology service providers who may be located in the United States of America.

Where Sundale discloses personal information overseas, Sundale will take reasonable steps to ensure overseas recipients handle personal information in a manner consistent with Australian privacy requirements unless an exception under the Privacy Act applies. Workers acknowledge that some information may be processed by overseas service providers supporting Sundale's technology and business operations. Further information regarding overseas disclosures may be provided in applicable Privacy Collection Statements or notices.

Security

Sundale implements reasonable technical and organisational measures to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. Such measures may include access controls, security monitoring, encryption, multi-factor authentication, staff training, secure disposal practices, incident response processes and regular risk assessments.

Personal information collected is wherever possible hosted on third party data servers located within Australia. Sundale takes reasonable steps to ensure these third-party data storage suppliers Sundale partners with have appropriate cyber and physical security controls in place. Where personal information held is no longer necessary for Sundale's operations, it deletes information or permanently de-identifies it, subject to specific laws in respect of data retention.

Data Breaches

Sundale maintains procedures for identifying, assessing and responding to actual or suspected privacy incidents and eligible data breaches. Where required by law, Sundale will notify affected individuals and regulatory authorities of eligible data breaches. Workers must immediately report any actual or suspected privacy incident or security incident in accordance with Sundale's Data Breach Reporting and Response Procedure.

Closed Circuit Television (CCTV) surveillance

CCTV refers to camera surveillance that captures images of people and activity. Any personal information collected through CCTV surveillance must comply with the Privacy Law.

CCTV operates in some common and/or external areas of certain Sundale premises. The main purpose of this is to maintain a safe and secure environment for our employees, clients, residents and visitors. We may use personal information gathered from CCTV for security, risk management and incident investigation purposes. Access to CCTV footage will only be granted where access is required or authorised by law.

Access and correction

Workers may access the personal information Sundale holds about them upon making a written request. After verifying their identity, Sundale will respond to a request within a reasonable

period, and endeavours to respond to requests within 30 calendar days unless a longer period is permitted by law or reasonably required due to the complexity of the request. Sundale will not charge any fee for a request for access but may charge a fee of $0.20 per A4 page for processing any request for hard copy records, in addition to the cost of postage.

Subject to Sundale's obligations under the FW Act, Sundale may decline a request for access to personal information in circumstances prescribed by the Privacy Act, and if it does, it will give the worker a written notice that sets out the reasons for the refusal (unless it would be unreasonable to provide those reasons), including details of the mechanisms available to make a complaint.

Employee records prescribed by the FW Act must be made available to an employee or their representative upon request. These employee records include general employment details, pay records, records relating to leave entitlements, records relating to superannuation contributions, records relating to individual flexibility arrangements, records relating to guarantees of annual earnings, and termination of employment records.

Under the FW Act, Sundale must make a copy of an employee record available in a legible form for inspection and copying on request by an employee or former employee to whom the record relates. If the employee record is kept at the premises at which the employee works or the former employee worked, Sundale will make a copy available at the premises within three (3) business days after receiving a request or will post a copy of the employee record within 14 days after receiving a request. If the employee record is not kept at the premises, Sundale will, as soon as practicable after receiving a request, make a copy available at the premises or post a copy of the employee record to the employee or former employee. This provision does not apply to all workers, as not all workers are employees of Sundale.

It is essential that the information contained in Sundale's records is accurate, complete, and up to date. If a worker, upon receiving access to its personal information or at any other time, believes the personal information Sundale holds about the worker is inaccurate, incomplete, or out of date, the worker must notify Sundale immediately. Sundale will take reasonable steps to correct the information so that it is accurate, complete, and up to date.

If Sundale refuses to correct a worker's personal information, Sundale will give a written notice that sets out the reasons for refusal (unless it would be unreasonable to provide those reasons), including the mechanisms available to make a complaint.

Sundale's expectations of workers

In addition to Sundale's privacy obligations to workers, Sundale has obligations to all individuals whose personal information it collects, holds, uses, and discloses.

Workers are required to comply with this Policy to enable Sundale to comply with its obligations, minimise legal risks to Sundale and mitigate risks of the loss, unauthorised access, modification or disclosure of personal information. Workers must be prompt and forthright in reporting any actual or suspected breaches of privacy.

Workers with supervisory and governance responsibilities must also demonstrate and encourage behaviours in compliance with this Policy and assist workers to understand their obligations under the Applicable Laws.

Collection of personal information

In general terms, workers must only:

(a) ask for personal information relevant to Sundale's business or actual or potential relationship with an individual;

(b) collect personal information where it is necessary for, or directly relevant to, one or more of Sundale's functions or activities; and

(c) collect the personal information by fair and lawful means.

When collecting personal information, workers must:

(a) collect it from the individual directly (for example when they provide it by phone, letter, electronic form, or in other documents), unless it is impractical to do so, in which case the individual concerned should be notified of that collection before, or at the time of, collection or, if that is not possible, as soon as practicable after collection; and

(b) provide the individual with Sundale's *Privacy Collection Statement* (QA-200-P-31). Where information is collected over the phone, the worker is required to read out the Privacy Collection Statement script.

Individuals may request access to the personal information held about them. Any such requests must be referred to the Privacy Officer.

If personal information has been provided to Sundale and that information has not been requested, workers must consider whether the information could have been collected in accordance with this Policy and, if not, destroy or de-identify the personal information as soon as practicable.

Using personal information

Workers must only use personal information (particularly personal information of Customers) for the purposes for which it was collected as set out in the applicable Privacy Collection Statement, as well as in Sundale's Customer privacy policy.

Workers may also use and disclose personal information (other than the personal information of a customer) for a secondary purpose if:

(a) the individual has consented to the secondary use or disclosure;

(b) the individual would reasonably expect Sundale to use or disclose their personal information for the secondary purpose, which is related to the primary purpose of collection; and

(c) the secondary use is otherwise required or authorised by law, or under an Australian court or tribunal order.

Direct marketing and privacy

Workers may not use the personal information of Customers for direct marketing purposes.

Workers may only use other individuals' personal information for direct marketing if the individual received a copy of the Privacy Collection Statement at the time of collection or would otherwise reasonably expect their personal information to be used by Sundale for the purposes of direct marketing.

Individuals can 'opt out' of Sundale's direct marketing by notifying Sundale that they do not wish to receive this material.

For all digital direct marketing communications, the communication must draw attention to the individual's opt-out rights with a simple and easy-to-use unsubscribe function.

Workers should ensure that any requests to unsubscribe are addressed in a timely fashion, and in any event, within 5 business days.

Disclosing personal information

Workers must only disclose personal information for the purposes for which it was collected as set out in the applicable Privacy Collection Statement, as well as in Sundale's Customer privacy policy.

Except with respect to personal information of Customers, workers may generally also disclose personal information for a secondary purpose if:

(a) the individual has consented to a secondary disclosure;

(b) the individual would reasonably expect Sundale to disclose their personal information for the secondary purpose (such as when notified of a secondary purpose in a Privacy Collection Statement), and that purpose is related to the primary purpose of collection, or in the case of Sensitive Information, directly related to the primary purpose;

(c) a 'permitted general situation' exists in relation to the secondary disclosure; a 'permitted general situation' includes: the lessening of or preventing a serious threat to the life, health, or safety of an individual, or to public health or safety; taking appropriate action in relation to suspected unlawful activity or serious misconduct; locating a person reported as missing; asserting a legal or equitable claim; and conducting an alternative dispute resolution process;

(d) a 'permitted health situation' exists in relation to the secondary disclosure; a 'permitted health situation' includes: the collection of health information to provide a health service; the collection of health information for certain research and other purposes; the use or disclosure of health information for certain research and other purposes; the use or disclosure of genetic information; and the disclosure of health information for a secondary purpose to a responsible person for an individual;

(e) it is reasonably believed that the secondary disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Workers must not disclose personal information to an overseas recipient unless the disclosure is authorised by law, consistent with Sundale's Privacy Collection Statement and Privacy Policy, and any applicable requirements relating to overseas disclosures have been satisfied. Where

required, reasonable steps must be taken to ensure overseas recipients handle personal information in a manner consistent with Australian privacy requirements.

Personal information of Customers may only be disclosed:

(a) with the written consent of the person;

(b) for a purpose connected with the provision of care by an approved provider;

(c) for a purpose for which it was provided to Sundale;

(d) for a purpose connected with the provision of aged care by another approved provider, so far as the disclosure relates to the individual's refundable deposit balance or accommodation bond balance or the period for which retention amounts may be deducted under section 57-20 of the *Aged Care (Transitional Provisions) Act 1997* or to the person's remaining liability (if any) to pay an accommodation payment, accommodation contribution or accommodation charge (as defined by the Aged Care Act); or

(e) for a purpose connected with the provision of aged care by another approved provider, so far as the disclosure relates to an appraisal or reappraisal connected with a classification that is in force for a care recipient to whom subsection 27-4(5) of the Aged Care Act applies (entry into another aged care service within 28 days);

(f) for the purpose of complying with an obligation under the Aged Care Act or the *Aged Care (Transitional Provisions) Act 1997* or any of the Principles made under section 96-1 of the Aged Care Act or the *Aged Care (Transitional Provisions) Act 1997*; or

(g) to a court, tribunal, or other authority as required or authorised by law.

Under the Aged Care Act, it is an offence to make a copy of, disclose, or otherwise use personal information in a manner that is not authorised. Penalties include imprisonment for two years.

Consent

Consent **is** required:

(a) to collect Sensitive Information, or

(b) to use or disclose personal information for a purpose other than the purpose it was collected for (unless an above exemption applies).

Consent may be express or implied. Express consent must be provided voluntarily, current and specific and the individual must be informed of what they are consenting to and have the capacity to understand and communicate their consent. Implied consent can only be relied on if the individual has been provided with an opportunity to opt out of consenting.

Workers must not engage in 'consent bundling', where a single request for consent covers multiple requests to collect, use, and disclose and does not let the individual choose which ones they consent to and which ones they don't. In these circumstances, it is not possible to determine whether consent has actually been provided for all requests.

Consent may be revoked (which may cause difficulties for Sundale's internal operations), and so Sundale's policy is that where consent is not required, it should not be sought. Workers must cease using personal information if an individual has withdrawn their consent at any time.

Security

Workers must comply with all security policies, procedures, directions and protocols with respect to personal information for both physical and digital security.

Workers must also comply with Sundale's Acceptable Use Policy when using technology, systems and AI tools. In particular, Sundale information must only be created, analysed or processed using approved AI tools, including Microsoft Copilot when accessed through a Sundale-managed account, unless expressly authorised. Workers must not upload Sundale information, including personal, sensitive or classified information, to external or non-sanctioned AI tools. AI-generated content must be reviewed and validated before use, and any suspected misuse or anomalous activity must be reported to Sundale ICT.

Reportable assaults

The Aged Care Act sets out responsibilities for Sundale and its workers with respect to reportable assaults.

A reportable assault is any unlawful sexual contact, unreasonable use of force, or assault specified in the Accountability Principles, and constituting an offence against a law of the Commonwealth or a State or Territory, that is inflicted on a person receiving residential care.

Any worker who receives a report from another worker about a reportable assault **must not** disclose the identity of the reporting worker, except to one or more of: a police officer, the Quality

and Safety Commissioner, or a person, authority or court to whom Sundale is required to disclose the worker's identity, or one of Sundale's key personnel, such as a member of the Executive Leadership Team. The reporting worker must not be subject to any reprisal action.

Complaints

Individuals may make a complaint regarding Sundale's collection, use, disclosure, storage, security, retention, destruction or other handling of personal information. Complaints may also relate to employee monitoring, automated decision-making practices, data breaches, direct marketing activities or overseas disclosures.

In the first instance, the Privacy Officer will acknowledge that complaint within two (2) working days and notify the person making the complaint or enquiry of the name of the person responsible for investigating the matter.

Where a matter is not resolved within 10 working days, the Privacy Officer will contact the person making the complaint or enquiry and inform them as to its progress and status and when Sundale expects the matter to be resolved.

If, after this process, the person making the complaint or enquiry is not satisfied with Sundale's response, they can submit a complaint to the Office of the Australian Information Commission (**OAIC**) www.oaic.gov.au or on 1300 363 992 To lodge a complaint, visit the 'complaints' section of the OAIC's website to obtain the relevant complaint form, or contact the OAIC's office.

Who is Responsible for Managing Your Information?

Sundale's Privacy Officer is responsible for overseeing compliance with applicable privacy laws, monitoring privacy risks, coordinating privacy training and awareness activities, supporting privacy impact assessments, managing privacy incidents and eligible data breaches, and facilitating responses to privacy complaints and regulatory enquiries.

If you have any questions, concerns, or would like to make a privacy complaint, please

contact the Privacy Officer:

Email: privacy@sundale.org.au

Phone: 1800 786 325

Breaches and reporting

The law imposes strict requirements and deadlines in relation to the actions that Sundale has to take in the event of an actual or suspected data breach (when personal information held by Sundale is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference).

Any actual or suspected data breach must be immediately reported to the Privacy Officer and any other required persons in accordance with Sundale's Data Breach Reporting and Response procedure.

Review of and access to this Policy

This Policy will be reviewed by the Board at least every two years, and sooner where there are material changes to legislation, regulatory guidance, organisational practices, technologies, or privacy risk exposures.

A copy of this policy will be available to workers on Sundale's intranet.

Breach of Policy

It is each worker's responsibility to act in a manner consistent with the spirit, intent and requirements of this Policy.

If a worker is found to have performed or engaged in behaviour in a deliberate breach or repeated breaches of this Policy, the worker may be subject to disciplinary action, which may include:

(a) for an employee, termination of the employee's employment with Sundale;

(b) for volunteers or unpaid work experience students, termination of the person's engagement with Sundale;

(c) for contractors, consultants or labour hire workers, termination of the person's services;

(d) for a Board member, resignation or other disciplinary procedures determined by the Board (other than the board member).

Sundale appreciates that accidents happen and mistakes are made. If a worker becomes aware of an accident or mistake that has led to a breach of this policy, it is very important to report it immediately in accordance with the breach and reporting procedures so that Sundale can take

appropriate actions to remediate the situation and reduce the risk of liability to Sundale for a privacy breach.

The disciplinary actions set out above are intended to apply to deliberate breaches of this policy or repeated acts / omissions which show a complete disregard of privacy obligations.

The disciplinary actions are not intended to apply to accidents and mistakes, and there will be no disciplinary actions or reprisals for workers who make these reports.

Definitions

Aged Care Act: means the *Aged Care Act 2024 (Cth)*.

Applicable Laws:

Applicable Laws means:

- Privacy Act 1988 (Cth);
- Australian Privacy Principles;
- Privacy and Other Legislation Amendment Act 2024 (Cth);
- Aged Care Act 2024 (Cth);
- Fair Work Act 2009 (Cth);
- Fair Work Regulations 2009 (Cth); and
- any other legislation, standards, regulations or legally binding requirements applicable to the handling of personal information.

Automated Decision-Making: Means a decision, or a process substantially and directly related to making a decision, that uses a computer program and personal information and that could reasonably be expected to significantly affect the rights or interests of an individual.

Board: means the board of directors of Sundale.

Customer: means a person who receives, has received, or is seeking to receive services from Sundale, including residents, home care participants, clients, consumers and care recipients.

FW Act: means the *Fair Work Act 2009 (Cth)* and the *Fair Work Regulations 2009 (Cth)*.

Privacy Act: means the *Privacy Act 1988 (Cth)* and any regulations, Australian Privacy Principles, codes, determinations, guidelines or other instruments made under it, as amended from time to time.

Privacy Collection Statement: is a statement, notice or other document required by applicable privacy laws, including the Privacy Act and Australian Privacy Principles,

and includes:

(a) Sundale's identity and contact details;

(b) the facts and circumstances of collection;

(c) whether collection is required or authorised by law, and if so, the names of such laws;

(d) the purposes for which the information is collected;

(e) the consequences for the individual if Sundale does not collect the personal information;

(f) the third parties or the types of third parties to whom Sundale normally discloses personal information;

(g) that Sundale's public-facing privacy policy contains information about how customers may access and seek correction of their personal information, and complain about a breach of the APPs and how Sundale will deal with such a complaint; and

(h) whether Sundale is likely to disclose personal information to overseas recipients and, if so, the countries in which such recipients are located (if practical to specify).

(i) where applicable, information about the use of automated decision-making processes, including the kinds of personal information used and the kinds of decisions that may be made or substantially assisted by such processes.

Privacy Officer: means the person appointed by Sundale to oversee compliance with privacy obligations and manage privacy-related enquiries, complaints and incidents.

Sensitive information: means sensitive information as defined in the Privacy Act 1988 (Cth), including information about an individual's health, racial or ethnic origin, political opinions, religious beliefs, sexual orientation, criminal record, membership of a professional or trade association or trade union, genetic information, biometric information and biometric templates.

Resources and References

Internal

Code of Conduct and Ethics Policy

Privacy Collection Statement

Acceptable Use Policy

External

Aged Care Act 2024 https://www.legislation.gov.au/C2024A00104

Australian Privacy Principles https://www.oaic.gov.au/privacy/australian-privacy-principles

Privacy Act 1988 https://www.legislation.gov.au/Series/C2004A03712

PRIVACY: Sundale collects information according to the Privacy Act 1988 and the Australian Privacy Principles. A copy of our complete Privacy Policy is available on request or on our website.

This document is only current as at the time of printing and should not be relied upon as a current reference document. It is your responsibility to always refer to the Accreditation Portal for the latest version.

Version Control and Change History

Version	Approval Date	Reviewer/s	Amendment
1	29.06.2020	Sundale Board, Sundale Executive Managers, Policy & Procedure Manager, Corporate Lawyers	Review under current laws
2	09.07.2023	ELT and Sundale Board	Review currency
3	31.03.2025	ELT and Sundale Board	Review currency
4	27.07.2026	ELT, Governance & Risk Committee Sundale Board	Review currency – update legislation references, update to document number
5	26.10.2026	Sundale Board	Policy reviewed following Privacy and Other Legislation Amendment Act 2024 reforms and December 2026 privacy transparency requirements.