



Privacy and Confidentiality Policy

Version 7, January 2020





LivCor is committed to maintaining the privacy and confidentiality of its personnel and client records. LivCor undertakes to comply with the *Information Privacy Act 2000 (Vic)*, the *Privacy Act 1988 (Cth)* as amended including the 13 Australian Privacy Principles (APPs).



APP 1

Open and transparent management of personal information

LivCor retains a record of personal information about all individuals with whom we undertake any form of business activity. LivCor must collect, hold, use and disclose information from our clients and stakeholders for a range of purposes, including but not limited to:

- Providing products and services to clients;
- Managing employees, re-sellers and training partners;
- Promoting products and services;
- Conducting internal business functions and activities; and
- Meeting requirements of stakeholders.

Types of information collected

The following types of personal information may be collected, depending on the type of interaction and the requirements for the service LivCor is delivering:

- Device information, automatically collected through interaction with LivCor websites, which includes web browser, IP address, time zone, some of the cookies installed on the device and pages, products or training courses viewed;
- Product order information, used for client communication, to fulfill orders, screen for potential risk or fraud, and when in line with shared preferences, provide relevant, targeted information or advertising of LivCor products or services;
- Contact details;
- Employment details;
- Educational background;
- Demographic information;
- Course progress and achievement information; and
- Financial billing information.

The following types of sensitive information may also be collected and held:

- Identity details (name, date of birth) and Unique Student Identifier (USI);
- Employee details and HR information;
- Complaint or issue information;
- Disability status and other individual needs;
- Indigenous status;
- Background checks (such as criminal checks or working with children checks); and
- Copies of licences.

How personal information is collected

LivCor will usually collect any required information directly from the individuals concerned. This may include the use of forms (such as registration forms, enrolment forms, training partner application forms or re-seller application forms) and the use of web-based systems such as online enquiry forms, product order forms, training enrolment forms, web portals or information management systems. Device information is collected from visitors to the LivCor website using:

- cookies, which are data files placed on the visitor's device;
- log files that track actions occurring on the site;
- web beacons, tags and pixels that record information on how each visitor uses the site.

Note that the LivCor website's data collection and use practices are not altered by a do-not-track signal from a web browser.

How personal information is held

LivCor will use robust storage and security measures at all times. Information on collection is:

- As soon as practical, converted to electronic means;
- Stored in secure, password-protected systems, such as financial system, learning management system, student management system and customer relationship management system; and
- Monitored for appropriate authorised use at all times.

Only authorised personnel are provided with login information to each system, with system access limited to only those relevant to their specific role. LivCor ICT systems are hosted in secure cloud-based environments, with robust internal security to physical server locations and server systems access. Virus protection, backup procedures and ongoing access monitoring procedures are in place.

Destruction of paper-based records occurs as soon as practicable in every matter, through the use of secure shredding and destruction services at LivCor head office.

Individual information held across systems is linked through a LivCor allocated identification number for each individual.

Disclosure to third parties

LivCor will not disclose information on clients or their participants enrolled in non-accredited training to any third party without the prior written permission of such clients or training participants.

As a registered training organisation (RTO), regulated by the Australian Skills Quality Authority (ASQA), LivCor is required to collect, hold, use and disclose a wide range of personal and sensitive information on clients and their participants enrolled in nationally-recognised training programs. This information requirement is outlined in the National Vocational Education and Training Regulator Act 2011, the Student Identifiers Act 2014 and other associated legislative instruments, in particular:

- Standards for Registered Training Organisations (RTOs) 2015;
- Data Provision Requirements 2012 as amended;
- Student Identifiers Regulation 2014;
- National VET Data Policy – November 2017.

Individuals are advised that due to legal requirements, LivCor discloses information held on individuals enrolled in nationally-recognised training for valid purposes to a range of entities including:

- Governments (Commonwealth, State or Local);
- Employers (and their representatives), schools, guardians; and
- other Registered Training Organisations.

Personal information from clients of LivCor products is shared with Shopify to power our online store. Details of how Shopify uses personal information may be found at <https://www.shopify.com/legal/privacy>. LivCor also uses Google Analytics to help understand how customers use its online store. Information on how Google uses personal information may be found at <https://www.google.com/intl/en/policies/privacy>. Customers can opt out of Google Analytics at any time here: <https://tools.google.com/dlpage/gaoptout>.

Retention and Destruction of Information

LivCor undertakes secure destruction of personal information records as soon as possible after required use and storage periods have ended.

Accessing and seeking correction of personal information

LivCor confirms all individuals have a right to request access to their personal information held and to request its correction at any time. Students are able to log in to the training management system at any time to update their details. Individuals may also request access to personal records by making contact with:

LivCor - Office Manager
Ph 1300 975 889
courses@livcor.com.au

A number of third parties, other than the individual, may request access to an individual's personal information. Such third parties may include employers, parents or guardians, schools, Governments and other stakeholders.

In all cases where access is requested, LivCor will ensure that:

- Parties requesting access to personal information are robustly identified and vetted;
- Where legally possible, the individual to whom the information relates will be contacted to confirm consent (if consent not previously provided for the matter); and
- Only appropriately authorised parties, for valid purposes, will be provided access to the information.

Complaints about a breach of the APPs or a binding registered APP code

If an individual believes LivCor may have breached one of the APPs or a binding registered APP Privacy Complaints Procedure in the first instance contact:

LivCor - Office Manager
Ph 1300 975 889
courses@livcor.com.au

Review and update of this Privacy and Confidentiality Policy

LivCor reviews this Privacy and Confidentiality Policy:

- On an ongoing basis, as suggestions or issues are raised and addressed, or as government-required changes are identified;
- Through our internal audit processes on at least an annual basis; and
- As a component of each complaint investigation process where the complaint is related to a privacy matter.

Whenever this policy is updated, changes to the policy are widely communicated to stakeholders internally through staff communications, meetings, training and documentation, and externally through publishing of the policy on LivCor's website and other relevant documentation for clients.

APP 2

Anonymity and pseudonymity

LivCor provides individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with us in relation to a particular matter, whenever practical. This includes providing options for anonymous dealings in cases of general course enquiries or other situations in which an individual's information is not required to complete a request.

Individuals may deal with us by using a name, term or descriptor that is different to the individual's actual name wherever possible. This includes using generic email addresses that does not contain an individual's actual name or generic user names when individuals may access a public component of our website or enquiry forms.

LivCor only stores and links pseudonyms to individual personal information in cases where this is required for service delivery (such as system login information) or once the individual's consent has been received.

Circumstances requiring identification

LivCor must require and confirm identification to support our clients' service delivery to individuals for nationally-recognised training programs. It is a condition of registration under the National Vocational Education and Training Regulator Act 2011 that we identify individuals and their specific individual needs on commencement of service delivery, and collect and disclose Australian Vocational Education and Training Management of Information Statistical Standard (AVETMISS) data on all individuals enrolled in nationally recognised training programs. Other legal requirements, as noted earlier in this policy, also require considerable identification arrangements.

There are also other occasions within our service delivery where an individual may not have the option of dealing anonymously or by pseudonym, as identification is practically required for us to effectively support an individual's request or need.

APP 3

Collection of solicited personal information

LivCor only collects personal information that is reasonably necessary for our business activities.

We only collect sensitive information in cases where the individual consents to the sensitive information being collected, except in cases where we are required to collect this information by law, such as outlined earlier in this policy.

All information is collected only by lawful and fair means.

We only collect solicited information directly from the individual concerned, unless it is unreasonable or impracticable for the personal information to only be collected in this manner.

APP 4

Dealing with unsolicited personal information

LivCor may from time to time receive unsolicited personal information. Where this occurs, we promptly review the information to decide whether or not we could have collected the information for the purpose of our business activities. Where this is the case, we may hold, use and disclose the information appropriately as per the practices outlined in this policy.

Where we could not have collected this information by law or for a valid business purpose we immediately destroy or de-identify the information unless it would be unlawful to do so.

APP 5

Notification of the collection of personal information

Whenever LivCor collects personal information about an individual, we take reasonable steps to notify the individual of the details of the information collection or otherwise ensure the individual is aware of those matters. This notification occurs at or before the time of collection, or as soon as practicable afterwards.

Our notifications to individuals on data collection include:

- LivCor's identity and contact details, including the position title, telephone number and email address of a contact who handles enquiries and requests relating to privacy matters;
- The facts and circumstances of collection such as the date, time, place and method of collection, and whether the information was collected from a third party, including the name of that party;
- If the collection is required or authorised by law, including the name of the Australian law or other legal agreement requiring the collection;
- The purpose of collection, including any primary and secondary purposes;
- The consequences for the individual if all or some personal information is not collected;
- Other organisations or persons to which the information is usually disclosed, including naming those parties;
- Whether we are likely to disclose the personal information to overseas recipients, and if so, the names of the recipients and the countries in which such recipients are located.
- A link to this Privacy and Confidentiality Policy on our website or explain how it may be accessed; and
- Advice that this Privacy and Confidentiality Policy contains information about how the individual may access and seek correction of the personal information held by us; and how to complain about a breach of the APPs, or any registered APP code, and how we will deal with such a complaint.

Where possible, we ensure that the individual confirms their understanding of these details, such as through signed declarations, website form acceptance of details or in person through questioning.

Where LivCor collects personal information from another organisation, LivCor will:

- Confirm whether the other organisation has provided the relevant notice above to the individual; or
- Whether the individual was otherwise aware of these details at the time of collection; and
- If this has not occurred, undertake this notice to ensure the individual is fully informed of the information collection

APP 6

Use or disclosure of personal information

LivCor only uses or discloses personal information it holds about an individual for the particular primary purposes for which the information was collected, or secondary purposes in cases where:

- An individual consented to a secondary use or disclosure;
- An individual would reasonably expect the secondary use or disclosure, and that is directly related to the primary purpose of collection; or
- Using or disclosing the information is required or authorised by law.

Requirement to make a written note of use or disclosure for this secondary purpose

If LivCor uses or discloses personal information in accordance with an enforcement-related activity we will make a written note of the use or disclosure, including the following details:

- The date of the use or disclosure;
- Details of the personal information that was used or disclosed;
- The enforcement body conducting the enforcement related activity;
- If the organisation used the information, how the information was used by the organisation;
- The basis for our reasonable belief that we were required to disclose the information.

APP 7

Direct marketing

LivCor does not use or disclose the personal information that it holds about an individual for the purpose of direct marketing, unless:

- The personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing; or
- The personal information has been collected from a third party, and the individual has a reasonable expectation that their personal information will be used for the purpose of direct marketing; and
- We provide a simple method for the individual to request not to receive direct marketing communications (also known as 'opting out').

As mentioned above under APP1, LivCor uses personal information to provide targeted advertising of LivCor products or services that may be of interest to specific clients. In each of our direct marketing communications, LivCor provides a prominent statement that the individual may request to opt out of future communications and all such messages will include an opt-out link.

An individual may also request us at any stage not to use or disclose their personal information for the purpose of direct marketing, or to facilitate direct marketing by other organisations. We comply with any request by an individual promptly and undertake any required actions for free.

We also, on request, notify an individual of our source of their personal information used or disclosed for the purpose of direct marketing unless it is unreasonable or impracticable to do so.

APP 8

Cross-border disclosure of personal information

LivCor does not disclose personal information on clients or staff to any overseas recipient. The only contact information provided to overseas service or product providers is company email addresses or telephone numbers.

LivCor will only disclose company contact information to overseas organisations where such contact is essential to the conduct of business and where the overseas organisation is subject to privacy laws in their own jurisdiction and have a privacy policy that forbids forwarding of company contact information to any third party.

APP 9

Adoption, use or disclosure of government related identifiers

LivCor does not adopt, use or disclose a government related identifier related to an individual except:

- in situations required by Australian law or other legal requirements;
- where reasonably necessary to verify the identity of the individual;
- where reasonably necessary to fulfil obligations to an agency or a State or Territory authority; or
- as prescribed by regulations.

APP 10

Quality of personal information

LivCor takes reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. We also take reasonable steps to ensure that the personal information we use or disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. This is particularly important when we:

- initially collect the personal information; and
- use or disclose personal information.

We take steps to ensure personal information is factually correct. In cases of an opinion, we ensure information takes into account competing facts and views and makes an informed assessment, providing it is clear this is an opinion. Information is confirmed up-to-date at the point in time to which the personal information relates.

Quality measures in place supporting these requirements include:

- Internal practices, procedures and systems to audit, monitor, identify and correct poor-quality personal information (including training staff in these practices, procedures and systems);
- Protocols that ensure personal information is collected and recorded in a consistent format, from a primary information source when possible;
- Ensuring updated or new personal information is promptly added to relevant existing records;
- Providing individuals with a simple means to review and update their information on an on-going basis through our online portal;
- Reminding individuals to update their personal information at critical service delivery points (such as completion) when we engage with the individual;
- Contacting individuals to verify the quality of personal information where appropriate when it is about to be used or disclosed, particularly if there has been a lengthy period since collection; and
- Checking that a third party, from whom personal information is collected, has implemented appropriate data quality practices, procedures and systems.

APP 11

Security of personal information

LivCor takes active measures to consider whether we are able to retain personal information we hold, and also to ensure the security of personal information we hold. This includes reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

We destroy or de-identify personal information held once the information is no longer needed for any purpose for which the information may be legally used or disclosed.

Access to LivCor offices and work areas is limited to our personnel only - visitors to our premises must be authorised by relevant personnel and are accompanied at all times. With regard to any information in a paper-based form, we maintain storage of records in an appropriately secure place to which only authorised individuals have access.

Regular staff training and information bulletins are conducted with LivCor personnel on privacy issues, and how the APPs apply to our practices, procedures and systems. Training is also included in our staff induction practices.

LivCor conducts ongoing internal audits (at least annually and as needed) of the adequacy and currency of security and access practices, procedures and systems implemented.

LivCor will also make all necessary preparations to be able to respond to any privacy data breach. Where unauthorised access or disclosure is detected, or information has been lost in circumstances where unauthorised access is possible, LivCor will promptly activate its Data Breach Response Plan.

LivCor's Data Breach Response Team is responsible for ensuring the plan is followed and for assessing and managing any breach and will determine whether the incident is an eligible data breach under the Notifiable Data Breach (NDB) scheme. The Data Breach Response Team is also responsible for delivering any notifications that may be required in a timely manner.

LivCor will take all reasonable steps to limit the consequences of a data breach and to preserve and build public trust in its management of personal information.

APP 12

Access to personal information

Where LivCor holds personal information about an individual, we provide that individual access to the information on their request. In processing requests, we:

- ensure through confirmation of identity that the request is made by the individual concerned, or by another person who is authorised to make a request on their behalf;
- respond to a request for access within 14 calendar days, when notifying our refusal to give access, including providing reasons for refusal in writing, and the complaint mechanisms available to the individual or within 30 calendar days, by giving access to the personal information that is requested in the manner in which it was requested;
- provide information access free of charge.

APP 13

Correction of personal information

LivCor takes reasonable steps to correct personal information we hold, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

On an individual's request, LivCor will:

- Correct personal information held; and
- Notify any third parties of corrections made to personal information, if this information was previously provided to these parties.

In cases where we refuse to update personal information, LivCor will:

- Give a written notice to the individual, including the reasons for the refusal and the complaint mechanisms available to the individual;
- Upon request by the individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading;
- Respond within 14 calendar days to these requests; and
- Complete all actions free of charge.

Correcting at LivCor's initiative

LivCor will take all reasonable steps to correct personal information in cases where we are satisfied that the personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading. This awareness may occur through collection of updated information, in notification from third parties or through other means.