

LCBA PRIVACY POLICY

1. Purpose and Objectives

- 1.1 This policy outlines how Le Cordon Bleu Australia (LCBA) uses and manages personal information provided to, or collected by, LCBA.
- 1.2 LCBA acknowledges its obligation with the collection, storage and use of information under the Privacy Act 1988, the Privacy Management (Enhancing Privacy Protection) Act 2012 and the Australian Privacy Principles (APPs) and the Privacy Amendment (Notifiable Data Breaches) Act 2017.
- 1.3 Due to the ownership of LCBA by a company established within the European Union (EU), LCBA is also bound by the General Data Protection Regulation (GDPR).
- 1.4 LCBA may, from time to time, review and update this LCBA Privacy Policy to ensure it is compliant with changing legal requirements and suitable for its operational context.

2. Scope

- 2.1 This Policy relates to the collection, storage, use and disclosure of personal information by LCBA, and applies to all prospective, past and present: staff, students, parents, guardians, agents, teachers, employers and industry partners in their association with LCBA, and including through the LCBA website and social media platforms.

3. Legislative Context

- 3.1 LCBA is obliged under various legislative frameworks to collect and submit data to government and regulatory agencies pertaining to the provision of education services. Such data may include personal information concerning students, staff, or otherwise relating to its programs, third party arrangements and other operational matters. Such legislative frameworks include (but are not restricted to) the following:
 - Australian Qualifications Framework (AQF) 2013.
 - Education Services for Overseas Students (ESOS) Act 2000.
 - Freedom of Information Act 1982 (FOI Act).
 - National Vocational and Education Training (VET) Regulator Act 2011.
 - Privacy Act 1988 (Cth) and Australian Privacy Principles (the APPs) from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012.
 - Tertiary Education Quality and Standards Agency (TEQSA) Act 2011.
 - Higher Education Standards Framework (Threshold Standards) 2021

Economic Union (EU)

 - General Data Protection Regulation (GDPR).

4. Policy Statement

- 4.1 LCBA is committed to ensuring that the rights to Privacy and protection of personal information are maintained in the course of its educational delivery and operations. As an organisation operating within Australia with its ownership having establishment within the European Union, LCBA is bound by both Australian and EU requirements for its handling of personal information. The LCBA Privacy Policy incorporates both the Australian and EU Privacy principles in the management, use and retention of personal information collected by LCBA in the course of its operations.

LCBA PRIVACY POLICY

- 4.2 LCBA will take reasonable steps, including through use of appropriate technical and organisational measures, to implement practices, procedures and systems to ensure compliance with its privacy obligations.

5. Policy

- 5.1 LCBA is committed to an open and transparent management of personal information that it is required to collect for both operational and regulatory purposes.
- 5.2 The LCBA Privacy Policy is guided by both the Australian Privacy Principles and the EU Principles relating to processing of personal data.
- 5.3 LCBA collects personal information through various means and for explicit and legitimate purposes and has procedures in place for rectifying inaccuracies and maintaining up to date data.
- 5.4 LCBA requests for personal and private information are relevant and limited to what is necessary for the purpose it is being processed.
- 5.5 Personal and private information is held in accordance with regulatory retention requirements and the purpose for which it was collected.
- 5.6 LCBA implements practices, procedures and systems to ensure compliance with privacy laws, to protect personal data against unauthorised access, damage or loss, and to appropriately manage any enquiries or complaints about privacy.
- 5.7 To ensure the protection and integrity of the collected data, LCBA reserves the right to modify or update this LCBA Privacy Policy at any time without notice, in order to address changed circumstances or legislation, or improve data management practices.
- 5.8 LCBA will report an 'eligible data breach' to the Office of the Australian Information Commissioner (OAIC) and any affected individuals.

Collection of Personal Information

6. Type of information collected

- 6.1 LCBA may collect personal information, including sensitive information, about:
- current and potential students;
 - parents and/or guardians;
 - former students, graduates and alumni;
 - staff members, volunteers and contractors;
 - potential employers and industry partners;
 - agents, school professionals; and
 - individuals submitting a request to LCBA directly or through accessing the LCBA website.
- 6.2 Personal information, such as an individual name, address or email address, is not generally collected when accessing LCBA digital and social media sites or when only visiting the LCBA website.
- 6.3 However, in order for an individual to obtain information about LCBA, to register on a mailing list, or to proceed with an on-line application for an LCBA course, certain personal information including credit card information (if applicable) may be requested.

LCBA PRIVACY POLICY

- 6.4 LCBA information management systems retain student details as per Australian legislative requirements which require LCBA to request that students access and update certain details via online services.
- 6.5 Certain information may be recorded through the normal operation of LCBA's internet servers. In order to help administer the site and enhance the online experience, servers may gather information pertaining to the type of browser or operating system being used or the IP address of the user.
- 6.6 Computer facilities are provided on campus for student and staff. While LCBA's interest is to prevent illicit, illegal and excessive usage, computer users should be aware that LCBA and/or its co-delivery partners may monitor computer usage, including the sites visited and the items downloaded.

7. Method of Collection

- 7.1 LCBA will generally collect personal information by way of forms filled out by parents or students; in face-to-face meetings; during interviews; via telephone calls and through Internet or email enquiries.
- 7.2 In some circumstances, LCBA may obtain personal information about an individual from a source other than the individual or parent/guardian. Examples include reports provided by medical professionals, educational agents, another school, or information contained in industry newsletters and journals.
- 7.3 Where it does not contravene a regulatory requirement or impede business operations, individuals will be provided with the option of anonymity, either through not having to identify themselves or through using a pseudonym.

8. Purpose of Data Collection

- 8.1 LCBA will use personal information it collects from current past and potential students, parents and guardians, job applicants, staff members and contractors, education agents, teachers, employers, potential employers and Industry partners for the relevant primary purpose including:
- communicating with potential students, students and graduates, about matters related to them and their studies;
 - maintaining student records as per legislative requirements;
 - fulfilling legislative and regulatory requirements with respect to student welfare, data collection and provision to government and regulatory bodies;
 - responding to queries or requests for information in accordance with Privacy principles;
 - providing education and related services;
 - administering processes in regard to employment and contracts;
 - maintaining records of (potential) employers and industry partners accepting students as part of the cooperative education process;
 - satisfying insurance requirements;
 - distributing promotional material and marketing for the school.

LCBA PRIVACY POLICY

- 8.2 LCBA may also use personal information it collects for such other purposes that are related and are reasonably expected, or for which consent has been obtained at the time of collection.
- 8.3 LCBA publications, such as newsletters and magazines, may incorporate personal information including images. LCBA will obtain an individual's consent before using their image in a publication.

9. Access to Personal Information by Third Parties

- 9.1 Where a request for access to personal information is made by a third party, LCBA will seek consent from the relevant individual, unless disclosure of personal information is required or permitted by law, or which becomes public knowledge other than by a breach of law.
- 9.2 Generally, LCBA will refer requests for personal information of an individual to the individual for consent. In such cases, information will not be released without specific approval from the individual.

10. Disclosure of Personal Information

- 10.1 Disclosure of personal information is dependent upon the obligations of LCBA to disclose to regulatory authorities, the nature and relevance of the information, and the legitimacy of the purpose for disclosure. Wherever possible, LCBA will seek consent from the individual.
- 10.2 Sensitive information will be used and disclosed only for the purpose for which it was provided or for a directly related secondary purpose, unless agreed otherwise, or the use or disclosure of the sensitive information is allowed or required by law.
- 10.3 As part of an education provider's regulatory or legal requirements, LCBA may need to disclose personal information, including sensitive information, held about an individual to government departments without specific consent.
- 10.4 Under its obligations with the Education Services for Overseas Students Act (ESOS Act) 2000 and the National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students (the National Code), LCBA may provide personal information collected during the enrolment process to Commonwealth and State agencies and the Tuition Protection Service (TPS) and the TPS Director.
- 10.5 LCBA may disclose your personal information to Australian Government agencies including Services Australia, where this is required or authorised by Australian Law. Information about your enrolment with LCBA may be disclosed if you are claiming or receiving a payment from Services Australia. You are required to notify Services Australia of any change in circumstances that may affect your payment. All personal information disclosed to Services Australia is protected by the Privacy Act.
- 10.6 LCBA may disclose personal information to overseas recipients if it is required to fulfil the purpose for which it was collected, in which case LCBA will take reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles. LCBA is part of the global Le Cordon Bleu group of companies, and in the course of LCBA's business activities personal information may be transferred, accessed, processed and stored in various overseas countries.
- 10.7 LCBA may also disclose personal information to certain contractors or subcontractors that provide administrative, promotional or other services to LCBA.

LCBA PRIVACY POLICY

10.8 An individual may provide consent for a single request, or to instigate an authorisation for other parties to have access to their personal information. For example, students may authorise access to their parents or guardians for academic results.

10.9 LCBA may disclose personal information, including sensitive information, that the individual authorises, including to:

- another LCB school;
- parents/guardians, education agents, or other parties;
- sponsors;
- medical practitioners;
- potential employers and industry partners; or
- for the purposes of publication in newspaper, newsletters and magazines;
- surveys, research or other.

10.10 LCBA will not adopt a government-mandated student identifier as its own identifier of the student, or otherwise use a government-mandated student identifier, unless an exception applies or is required or authorised by or under an Australian law or a court/tribunal order.

11. Management, Security and Retention of Personal Information

11.1 Personal information collected by LCBA is stored in an appropriately secure format and held for operational and archival purposes. When personal information is no longer required for the purposes for which it was collected, it is deleted once any retention periods that apply have been observed.

11.2 LCBA retains personal information as long as it is required to fulfil its purpose and meet legal obligations. Once the data is no longer needed it is securely deleted. This process is managed by the IT department.

11.3 LCBA ensures transparency in its cross-border data transfers, taking all reasonable steps to confirm that personal information shared or stored overseas complies with Australian and international privacy laws. All transfers are conducted securely and solely for legitimate business and operational purposes.

11.4 LCBA staff are required to ensure the privacy of individuals and observe the confidentiality of personal information held by LCBA.

11.5 LCBA employs technical measures to prevent loss, unauthorised access or unintended use of information collected and held by LCBA. These include permission level access and password protections for digital records.

11.6 LCBA will take reasonable steps (including via regularly scheduled calls for individuals to update personal information) to ensure that the information held on file is accurate and complete. Where possible (see clause 13), LCBA will amend its records when personal information held is inaccurate, out- of-date, incomplete, irrelevant or misleading.

12. Data Breaches

12.1 LCBA will act to address any privacy breach as early as possible from notification of a breach event being reported.

LCBA PRIVACY POLICY

12.2 Personal Information accessed in a data breach includes names, addresses, dates of birth, phone numbers, personal email addresses, emergency contact details, tax file numbers, payroll information, bank account details, passport details and student academic records.

12.3 Some kinds of personal information breaches are more likely than others to cause serious harm e.g., Breaches that involve combinations of different types of personal information such as sensitive information (e.g., medical or health information), or documents commonly used for identity theft (e.g. drivers licence or passport information) or financial information are more likely to result in serious harm.

12.4 A privacy breach which is reasonably likely to result in serious harm to an individual may result from:

12.4.1 not meeting the legal obligations in relation to the collection, handling, use or disclosure of personal information; or

12.4.2 unauthorised access to or disclosure of personal information including events of 'hacking'; or

12.4.3 information being lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur.

12.5 LCBA will report within the legally required time frames, an 'eligible data breach' to the Office of the Australian Information Commissioner (OAIC) and to any affected individuals.

Doxing Prevention

LCBA strictly prohibits the unauthorised disclosure of personal information including acts of doxing, which involve maliciously publishing or sharing personal or sharing personal details online without consent. LCBA employs robust measures to safeguard personal data and will address any instances of doxing in accordance with legal requirements. Reports of doxing are to be directed to the Legal and Compliance Manager in the first instance.

13. Access to Personal Information

13.1 An individual may request access to their personal information held by LCBA to:

- check the accuracy of information and if required, to advise LCBA of any perceived inaccuracy.
- discover how their personal information has been handled or processed.
- make a formal request to have personal information deleted. These requests will be considered by the Legal and Compliance Manager.

13.2 Requests and enquiries to access, update or correct personal information can be directed to australia-compliance@cordobleu.edu. An individual will not be charged any cost for access to their personal information.

13.3 LCBA will require verification of identity before providing access to personal information. In some circumstances access and/or the request may be denied. Such circumstances include where doing so is permitted by law or where LCBA considers that the release of the information would have an unreasonable impact on the privacy of others.

13.4 If an individual believes that a breach of their privacy has occurred, they are encouraged to contact LCBA at australia-compliance@cordobleu.edu to discuss their concerns. All issues

LCBA PRIVACY POLICY

and/or complaints will be initially considered and dealt with by the Compliance Office and decisions made to escalate the matter internally or externally as required.

13.5 Individuals not satisfied with the outcome of their concern or complaint in accessing or amending their personal information are entitled to make a complaint to the Office of the Australian Information Commissioner (www.oaic.gov.au).

13.6 LCBA recognises the statutory tort for serious invasions of privacy under Australian law and is committed to preventing any breaches that may result in harm to individuals. LCBA ensures compliance with legal obligations to safeguard personal information and provides mechanisms as listed above for individuals to seek remedies.

14. Roles and Responsibilities

Roles	Responsibilities
Legal and Compliance Manager	Act as Data Protection Officer and Privacy Officer for LCBA in conjunction with HR Office. Manage issues and/or complaints regarding personal information data collection and management.
Corporate Board	Approval authority for publication of the Policy.
LCBA staff	Responsibility for ensuring personal data within Departments is treated confidentially.

15. Definitions

‘Consent’ means consent that is freely given, specific and informed, and provided by an individual who has been provided with adequate information and has sufficient capacity to understand and communicate consent.

“doxing” refers to the act of publicly sharing or publishing someone’s private or personal information online without their consent, typically with malicious intent

‘Government related identifier’ of an individual is defined as an identifier that has been assigned by: an agency; a State or Territory authority; an agent of an agency, or a State or Territory authority, acting in its capacity as agent, or a contracted service provider for a Commonwealth or a State contract. (6 (1) of the Privacy Act)

A **statutory tort** is a civil wrong that arises from a breach of duties or obligations explicitly established by legislation

‘Unique Student Identifiers’ (USI): Passport, Medicare, Centrelink reference and driver licence numbers are examples of government related identifiers.

‘Personal information’ means information or an opinion about an identified or identifiable individual:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

‘Privacy breach’ is an eligible data breach if it results in:

- Unauthorised access to or disclosure of personal information; or

LCBA PRIVACY POLICY

- Information being lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur, and this is reasonably likely to result in serious harm to an individual.

‘Sensitive information’ means information or an opinion about the ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices or criminal record that is also personal information, or health information, genetic information, biometric information or biometric templates of an individual.

‘Serious harm’ can include identity theft and serious physical, psychological, emotional, financial or reputational harm.

16. Related Documents

- Student Complaints and Appeals Policy
- Enrolment Policy

17. Implementation

17.1 The Compliance Office is responsible for ensuring that future major changes to this policy will be accompanied by a completed Implementation Plan, presented with the policy to the Corporate Board.

17.2 The Implementation Plan will include a Communication Strategy that identifies key stakeholders and the requirements for effectively implementing and monitoring this policy.

18. Summary of changes since last review

Authored by	Description
Legal and Compliance Manager	<ul style="list-style-type: none"> Update in terminology benchmarked against other providers. Update in job titles
Legal and Compliance Manager	<ul style="list-style-type: none"> Update due to changes in the Privacy Act from December 2024.