

The Pet Industry College (RTO 70236), Agribusiness Industry College and Equine Industry College

Privacy Policy and Procedure

Version: 2.0

Review: Annually

Owner: National Education Manager

Approved by: CEO

1. Purpose

This policy outlines how JSBIGGS Pty Limited (ABN 69 082 974 936) and JSBIGGS Holdings Pty Limited (ABN 96 634 532 764), trading as **The Pet Industry College, Agribusiness Industry College and Equine Industry College** (together 'the College'), collect, store, use, disclose, protect and dispose of personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Standards for Registered Training Organisations (RTOs) 2025, the Student Identifiers Act 2014 and other applicable legislation.

All three trading names operate under, and are governed by, the same company and this policy applies equally to each of them.

2. Scope

Applies to all students, prospective students, staff, contractors, volunteers and third-party service providers of the College, across all three trading names.

3. Policy

- Only information necessary for enrolment, training, assessment, support and regulatory reporting will be collected.
- Sensitive information will only be collected where authorised by law or with consent.
- Information is collected through administrative tools such as the Enquiry Form, Enrolment Form, Recognition of Prior Learning Application Form, Credit Transfer Form, Complaint Form, Appeals Form, Payment Refund Form, surveys, questionnaires and completed assessment submissions.

- Information is used for training delivery, assessment, student support, issuing qualifications, regulatory reporting (including AVETMISS), funding administration and legal obligations.
- Personal information relating to a student's enrolment is retained for up to 30 years, including personal details and training and assessment outcomes, in accordance with the National Vocational Education and Training Regulator (NVETR) Act 2011.
- Personal information and training/assessment activity is entered and retained within the College's secure computer network and software systems, protected and backed up frequently to a secure server located in Australia. Where information is collected in hard copy, it is entered into the College's systems, reviewed and/or analysed as required, and the hard copies are then destroyed.
- Personal information will not be disclosed except where authorised by the individual, required by law, or required by government agencies or regulators — including the National Centre for Vocational Education and Research (NCVER), the Australian Skills Quality Authority (ASQA), or any relevant State or Territory Training or Funding Authority.
- Under the National Vocational Education and Training Regulator (Data Provision Requirements) Instrument 2020, the College is required to collect and disclose personal information to NCVER, which may use and disclose it to the Department of Education, Skills and Employment, Commonwealth, State and Territory authorities, and VET regulators, to enable: populating authenticated VET transcripts; administering vocational education and training; facilitating statistics and research; and understanding the VET market. NCVER may also disclose information to persons it engages to conduct research on its behalf; NCVER does not intend to disclose personal information to overseas recipients. See NCVER's own Privacy Policy for further detail.
- Students may receive a student survey run by a government department, NCVER, or another authorised agency, and have the right to opt out at the time of being contacted.
- Reasonable technical and organisational controls protect information against loss, unauthorised access, misuse or disclosure.
- Where a third party requests personal information, the College will seek written permission before disclosing it — except where an employer or job network provider that has paid for training requests activity information and outcomes, where an organisation such as a Compliance Consultant requires it for the College's operations, or where disclosure is required by law (e.g. to ASQA or NCVER).
- Where the College receives unsolicited personal or sensitive information, it is treated and managed in accordance with the Australian Privacy Principles.
- **Our Website**
 - The College's website includes an Enquiry Form and other tools through which visitors may provide personal information, as described above.
 - The College uses Google Analytics and Cookies on its website to track and report website traffic and better understand visitors and users. Cookies are stored on

Google's servers in the United States and may be transferred to third parties if required by law, or for processing on Google's behalf. No personal information is recorded through this process; it is used only for website management and improvement. Visitors can disable cookies via their browser settings and opt out of Google Analytics, though this may affect their experience on the website.

- WordPress.org is used as the College's website content management platform.
- The College uses third-party and integrated products and systems which may require consent to use personal information, or which require personal information including name, address, contact details and financial information. These include, but are not limited to:
 - eSkilled Pty Ltd (Australia) — student management and learning platform. Privacy Policy: <https://rtosoftware.eskilled.com.au/privacy-policy/>
 - Go High Level LLC (GoHighLevel) — customer relationship management (CRM) platform. Data Processing Agreement: <https://www.gohighlevel.com/data-processing-agreement>
 - Stripe Payments Australia Pty Ltd (ACN 160 180 343) — payment processing. Data Processing Agreement: <https://stripe.com/au/legal/dpa>; Privacy Policy: <https://stripe.com/au/privacy>
 - Microsoft Corporation — email, document management and business productivity systems (including Microsoft 365 and SharePoint). Privacy Statement: <https://www.microsoft.com/en/trust-center/privacy>; Data Protection Addendum: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>

4. Student Rights

- Request access to personal information — via the online learning platform or by completing a Student Information Release Form, actioned within 2 business days.
- Request correction of inaccurate information, including legal name and contact details.
- Withdraw consent where legally permissible.
- Lodge a privacy complaint without disadvantage.

5. Data Breach Procedure

1. Contain the breach.
2. Assess the risk.
3. Notify affected individuals where required.
4. Notify the Office of the Australian Information Commissioner (OAIC) where required.
5. Investigate root cause and implement corrective actions.
6. Record the incident in the Data Breach Register.

6. Responsibilities

CEO: overall compliance.

National Education Manager: implementation and monitoring.

Staff: maintain confidentiality and follow this policy.

7. Related Documents

Records Management Policy; Complaints and Appeals Policy; Student Handbook; Data Breach Register.

Appendix A – Privacy Complaint Process

Complaints should be submitted in writing. Complaints will be acknowledged within 5 business days and investigated, with an outcome provided as soon as practicable. Under the Privacy Act 1988, individuals also have the right to make a complaint to the Office of the Australian Information Commissioner (OAIC) about the handling of their personal information by the College.