Computers4Learning Australian Privacy Principle privacy policy.

Computers4Learning (C4L) complies with these written Codes of Practice in the management of personal information of C4L business activities of the organization. Australian Privacy Principles (APP) tabled in Privacy Act 1988 - Schedule 1: encompass the what, where and why an organization handles personal information.

Australian Privacy Principles are:

APP 1 – open and transparent management of personal information.

C4L maintains organizational information data bases. As part of C4L business activities: the information is managed with complete openness and stored in the original form. C4L policy and procedures enable compliance: providing for individual enquiries or complaints via contact with management – Both oral and written forms of request are received and dealt with appropriately: this includes online access to contact C4L.
If the individual is unsatisfied with the results – complaint may be taken up with the Office of the Australian Information Commissioner: enquiries@oaic.gov.au further information at the Australian Government website of OAIC.
General Data collected by C4L will include details of all business activities. This is both internal and external information relevant to business activities and collected via both electronic and paper transfer of information and data. This will include personal data connected to C4L clients when products are purchased. Typically a name, address and contact details are collected.
Information stored by C4L: is held internally on an in-house Server at C4L site – that backs up to an external server on the Cloud service and is also backed up to extra internal storage at or near the workshop and some data is also backed up by portable devices controlled by management. The servers are protected by password access and general public encryption is applied to transfer of data across the internet. Portable storage drives, i.e. USB or external storage Hard Disk Drives or Solid State Drives are either password protected and/or the files are; which will be accountable for by the administrator that takes charge of them. Policies and procedures define data protection by design and by default.
At the time of collecting information or as soon as practicable, C4L will: ensure the individual understands how and why the information is collected - an online request of product form, at the C4Lwebpage fill-in form or paper form – which under certain circumstances may be processed at workshop. That the personal data collected is used to verify identity for approval and additionally to email a link to approved applicants for a web shopping page.
Clients are notified that some personal data are processed via third party agencies for sales recording and for financial transactions: as more commerce is transacted via online

platforms not controlled by C4L. That EFT payments are processed by third party agencies to invoice the client – if purchased directly online.
That Personnel information may be obtained by consent for internal record keeping and government compliance.
Which, if any information is disclosed to third party organizations.
That the C4L APP privacy policy contains information for the individual to access their personal information stored at C4L in a format usable by the individual.
How to make a complaint about breaches of the Privacy Act.
Or seek a correction to personal information held by C4L.
Whether C4L will disclosure personal information to overseas entities and which entities.

APP 2 – anonymity and pseudonyms.

C4L recognizes an individual's right to anonymity or a pseudonym when business dealings allow it. However registrations to third party services will require confirmable identification. For reasons of client legitimacy – C4L will not recognise anonymity when approving client request for products. This personal data is used to identify for validity and issue of receipt to client for products purchased and proof for warranty of products.

APP 3 – collection of solicited personal information.

The type of information C4L collects and holds is used in the business activities. Client, volunteer personnel, work experience attendee and contractor information is minimal and only necessary information is collected. The information will be obtained lawfully and by fair means. The information will only be obtained from the individual via consent – unless it is unreasonable or impractical to do so. This is compliant with part 2 of the schedule clause 3.4 (e) 1 & 2. 3.5, 3.6 (b).

APP 4 – dealing with unsolicited personal information.

If C4L receives personal information that it did not solicit: within a reasonable time period C4L will determine if the information would have been obtained for filing or information be de-identified or destroyed and deleted as irrelevant. If kept and filed: APP 5 – 13 may apply as solicited information obtained by C4L.

App 5 – notification of the collection of personal information.

At the time of collecting information or as soon as practicable, C4L will: identify and supply organization contact details. Ensures the individual understands how and why the information is collected. Any online forms C4L uses to collect client data at time of sale: will include clear affirmative consent via the ticking of check boxes, to indicate acceptance of conditions regarding sales: these are not prefilled and hold a nil value in standard machine readable format.
Notify if any information is disclosed to third party organizations: If C4L collects information for a third party entity, e.g. Microsoft End User Licence Agreement (EULA) C4L informs via written or verbal notification or both – so that the client is aware and understands that it is

such. Whether C4L will disclosure personal information to overseas entities and which entities.
How the C4L APP privacy policy contains information for the individual to access their personal information.
Make a complaint about breaches of the Privacy Act. Or seek a correction to personal information held.

App 6 – use or disclosure of personal information.

C4L will not use or disclose any personal information, other than for the purpose it was collected. Individuals consent and acknowledgement apply to any use or disclosure. Personnel data collection is for business activities compliance and internal staff management.
The information and Data collected by C4L for any business activities is only used for the prescribed purposes in the business dealings. Clients are notified and - will reasonably expect - that some personal data are processed via third party agencies for sales recording and for financial transactions. That EFT payments are processed by third party agencies to invoice the client – if purchased directly online: Computers 4 Learning makes use of 3rd parties to deliver some services. By using our services you are agreeing to our privacy policy and accepting that some personally identifiable information may be stored in 3rd party systems. The information and Data collected by C4L for any business activities is only stored in original format and never passed on to third party entities unrelated to the client sale. With client account data only held by C4L for processing purchases and qualifying criteria. Except where government regulations require the storage of certain records. Nor will C4L pass on personnel/compliance data or contract Memorandum Of Understanding (M.O.U.) statements – unless a government agency can show that it requires the information under regulated provisions. This will enforce C4L to comply with that directive.

APP 7 – direct marketing.

C4L business activities can include direct marketing to an individual that may be on file, e.g. customer satisfaction issues. However C4L will not disclose to third parties any personal information that may be used for the purpose of direct marketing: this includes sensitive personal information and non-sensitive personal information.

APP 8 – cross-border disclosure of personal information.

C4L will only disclose personal information in a cross-border situation if the individual understands the disclosure and gives consent. This would mean disclosure of personal data to another person not in Australia or Territory outside of Australian Law enforcement. C4L understands Clause 8.2 (a) 1&2 of the Schedule to apply in any cross-border disclosures –

C4L would understand similar protections as in APP and law enforcement would need to apply in any cross-border disclosure; so that subject data is adequately safeguarded.
This is the situation for the third party entity Microsoft and the End User Licence Agreement (EULA): compulsory when issued Microsoft products installed in C4L products.

C4L informs via written or verbal notification or both – so that the client is aware and understands that it is such.

APP 9 – adoption, use or disclosure of government related identifiers.

C4L will not use government identifiers in any part of the business activities record keeping associated with sales of products; if used as identity qualifiers: C4L will only keep a record for identification purposes, e.g. sighting of Driver's License, concession card, etc.
However; C4L will keep government identifiers when required by government agencies to maintain compliance to regulations. Specifically the recording and storage of copies - driver's license or other government identifiers when processing applications and maintaining Blue Card registrations for persons working with Children and Young people.

APP 10 – quality of personal information.

C4L will take all reasonable steps to ensure personal information is accurate, up to date, complete and relevant. The C4L Register of Documents: C4L Information & Data: Collection, Storage & Use of data – General & Personal Data Management – Policy & Procedure. S1:21. Contains management strategy taken to safeguard data integrity and correctness.

APP 11 – security of personal information.

C4L stores personal information in a secure and responsible manner. This ensures no misuse, interference, loss or unauthorized access and modification or disclosure. C4L will hold any personal information in such a manner: till the information is no long required for the purpose collected or any government regulation indicates - at which point, in a timely manner the personal information will be destroyed, de-identified or deleted.
C4L General Volunteer Code of Conduct requires all personnel to behave with respect in treating general data and personal information at the workplace and storage platforms used by C4L: relating to safeguarding the data.
All information both general and personal held at C4L workshop premises are protected against unauthorized access and use. Management restricts the access of general and personal data to approved personnel within the organisation and only for business related activities and processing. Security sensors and cameras monitor workshop premises during out of work hours.
C4L incorporates well designed and accredited web commerce platforms to conduct business activities. These Third Party entities are industry standard approved and develop practices to maximize security of the systems they control. As well as complying with the regulations and policies of the governing controlling bodies – Internet protocols for encryption and transmissions of data. Electronic Funds Transfer protocols are high level security processes regulated by government authorities.

APP 12 – access to personal information.

C4L will give access to an individual's personal information within a reasonable time, if a request is made by the individual. In that C4L is compliant with clause 12 of the Schedule.

Management will endeavour to supply the information as per requested or in a mutually acceptable means available. If C4L refuses to give access in relation to any of clause 12: C4L will give a written statement of reply to the effect of why access was denied.
Reasons for denial of request could be in cases where the information may impact on the privacy of other individuals, or be for a vexatious or frivolous access. If it is unlawful to do so: as it could impact on the rights and freedoms of other individuals. Or if C4L has reason to suspects that an unlawful activity will ensue if granted access to personal data.

APP 13 – correction of personal information.

If C4L is satisfied that personal information is in-accurate, or out of date, incomplete, irrelevant, misleading or the individual requests a correction of information: C4L will take all reasonable steps to correct the information. If the information was disclosed to a third party and the individual request that the third party be informed of the change: C4L will take all reasonable efforts to notify the third party. If C4L refuses to the personal information correction request: C4L will give a written statement as to why the request was denied. If the individual request that C4L give a written association that the information is incorrect: C4L will supply an association statement to the effect - so that the statement is apparent to users of the information. C4L will respond to any request in a reasonable time period.

For a complete listing of the Australian Privacy Principles see: Australian Government Privacy Act 1988 - Schedule 1.