CLEAR TO WORK PRIVACY POLICY

Clear to Work (CTW) takes the privacy of our students very seriously and we will comply with all legislative requirements. CTW Privacy Policy commits us to adhering to the legislative requirements set down by the Privacy Act 1988 (Cth), including the National Privacy Principles.

Student Records

Privacy & Access Guidelines apply to personal information collected, stored, and managed by CTW for internal use in connection with academic programs, and for the compilation of statistical reports to meet the requirements of relevant Departments of Education and Training, the Federal Department of Education and Training (www.education.gov.au), and National Centre for Vocational Education Research (NCVER) who use student data for statistical reports.
CTW stores student information in different ways, including hard copy documentation kept on individual student files and information kept electronically on the relevant student record database. This information will be kept confidential and will only be accessed by CTW staff that require such access to undertake their duties. Personal information will not be given to third parties outside CTW.

The limited exceptions to this are:

- Where the individual has provided written consent for disclosure.
- Where CTW is required or authorised to do so under Australian law including information to DEEWR with regards to the ESOS Act, National Code and Assurance Fund.
- Where the disclosure is judged to be in the clear interest of the individual (i.e., to prevent or lessen an imminent and serious threat to an individual's life or health).

If a student believes that the personal information is incorrect, inaccurate, or out of date, the student should advise CTW immediately so that reasonable steps may be made to correct the information.

If a student believes their personal information has not been dealt with in accordance with appropriate privacy principles, they may make a complaint to CTW seeking an internal review. A request for an internal review must be in writing and must be made within six months from the date when the suspected breach occurred.