Student Privacy

Procedure for Implementation

This procedure relates to the implementation of the Student Privacy Policy.

Procedure for Student to Access Personal Records:

1. The student will complete a Request to Access Personal Information form available from RTO Enrolment Officers.
2. The student will give or forward the completed form to the Manager Records and Reporting.
3. The RTO Enrolment Officers will then arrange a time with the student to view the contents of their personal file. The student will also be invited to view their file in the student management system (SMS).
4. The student will sign and date the Request to Access Personal Information form at the bottom to confirm that they have sighted their record.
5. A copy of this form is given back to the student and the original filed in the student's file.

Procedure for safeguarding confidential information obtained:

1. All staff are required as part of their employment contract to sign a Confidentiality Clause relating to student and organisational information.
2. All staff are given access, by the IT Manager, to selected areas (as required) of the Cire Training "Cloud" storage system.
3. Access to the electronic student management system is limited to authorised staff and is password protected. Usernames and passwords enabling access require pre-approval by the Executive Manager Education and Training and given by the authorised VETtrak Security User.
4. Current student files are kept in locked filing cabinets in the Administration Offices. Filing cabinet keys are available from authorised Administration Staff. Student files may only be accessed by the relevant Tutor/Trainer/Assessor and Education and Training Administration Staff.

Managing a data breach

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

Data breaches can be caused or exacerbated by a variety of factors and give rise to a range of actual or potential harms to individuals, agencies and organisations.

In the event of any suspected data breach, the matter will be investigated to determine:

- The nature of the breach.
- The number of people impacted.
- The nature of the breach and extent to which an individual or group may be harmed by the breach.
- Remedial action to minimise or prevent impact.
- Review of systems to minimise the possibility of future similar breach.

Related Policies and Procedures

Student Privacy Policy

Organisational Area

Cire Education and Training

Approved by:

The Board

Sign:..... Date: ...February...2019

Operative Date:

February 2019

Review Date:

February 2021