



Provider number 31430

IT and Information Security Policy (External)

1.0 Scope

This policy applies to all students at Churchill Education who utilise any of our IT services (Catapult, Office 365, etc).

2.0 Definitions

Credentials: your username and password

Office 365: the Microsoft service that allows access to Office Word, Office Excel, Office PowerPoint, Office Outlook, etc.

TFN: Tax File Number

Client/s: any person/s who have had, are having, or will prospectively have received training or interaction from Churchill Education.

3.0 Purpose

Your Churchill Education username and password grant you access to your Office 365 Mailbox, and other Office 365 services. You may also have access to services such Catapult – please apply this policy to these services as well.

This policy's objectives are

- To ensure security of the students' data from theft, malicious activity, breach of privacy.
- To protect Churchill Education from damage or liability arising from the use of our IT equipment for purposes contrary to Churchill Education Policies.
- To protect Churchill Education's students' data from falling into the wrong hands.

4.0 Creating and Maintaining Your Password

When you enrol in studies with Churchill Education, your user accounts will be created and provisioned for you by our Student Support Team. You will be given temporary credentials for our systems. Please be sure to change these passwords as soon as you log in for the first time.

When creating your password, follow the following guidelines:

- Do not use your first or last name
- Do not use your spouse's first or last name
- Do not use your birthdate or that of your spouse
- Minimum length of your password is nine (9) characters
- Must contain at least one of the following
 - o Capital
 - o Lowercase
 - o Number

5.0 Protecting Your Username and Password

Never respond to external emails asking you for your personal details such as:

- Username and password
- Date of birth
- Current address
- Bank account details
- Credit card details
- Tax File Number

Report suspicious emails that you receive to Grassroots IT (GRIT) at the following address: help@grassrootsit.com.au. This includes any emails that you suspect are illicit, spam, or could contain viruses that you've received at your Churchill Education email address.

Maintain the security of your Churchill Education username and password. Do not write your password down or disclose it to anyone else.

Knowingly disclosing passwords to others will be deemed a breach of policy and could be referred to disciplinary procedures. Churchill Education expects all students to adhere to this policy and take all reasonable steps to ensure the integrity and security of your Churchill Education managed IT accounts.

Please do not share your password with anybody, for your own security and that of Churchill Education's clients.

Churchill Education will never request:

- Your username or password via email;
- Personal information such as your username, password and bank details via email

6.0 Frequency of Password Changes

Your passwords must be updated frequently to protect against malicious activity such as damage, breach of privacy, etc. Users must change their password every ninety days. This goes for all services – Office 365, Catapult, etc. Users must not re-use a password that you have used in the last twelve (12) password changes.

7.0 Data Retention and Deleting Records

Please be aware that Churchill Education are required by ASQA to retain the records of students for thirty (30) years, as stated in *General Direction, Retention Requirements for Completed Student Assessment Items (ASQA, 2013)*.

Please be ensured that your student data will not be deleted, as this is a legal requirement.

8.0 Theft or Loss of Information or Equipment

If at any time you lose possession of your Churchill Education information either to theft or loss, please immediately notify your Mentor.

The following information will need to be noted:

- What exactly has gone missing?
- Was it lost or stolen, how do you know?

9.0 Copyright

Churchill Education, as with any business or individual, is expected to follow Australian copyright law. This law is governed by *Commonwealth Legislation – The Copyright Act 1968*.

There is to be no plagiarism (unauthorised copying of material) at Churchill Education from students or staff.

The Copyright Act does allow for some exemptions. These include:

- Research or study
- Criticism of review
- Reporting to the news
- Parody

Please note that your work will be checked for plagiarism and if found, you will be penalised.

10.0 Implementation

The Information Security Policy for Students is to be implemented to all Churchill Education Students via email when the student is enrolled.

11.0 Inappropriate Use

Use of Churchill Education IT resources must be work related and appropriate. Any inappropriate use of the IT systems at Churchill can result in punishment. Some inappropriate use may be considered a criminal offense under the *Criminal Code 1899 (QLD)*, for example *Section 408E, Computer hacking and misuse*.

Students must not replicate any information or content they receive from Churchill Education to a third party. This includes, but is not limited to:

- Training material

- Mentor contact details
- Passwords for accessing any Churchill Education systems or data

12.0 Questions

If a student is unsure about any matter covered by this policy, they should seek the assistance from their Mentor.

13.0 External Process

The above process does not replace or reduce any student's statutory rights.

14.0 Version Control

Version No.	Approval Date	Authorised By	Sections Modified and Summary of Changes
1.0	04/01/2016	Ross Caldwell	Created Student variation of original IT and Information Security Policy