Privacy Procedure

Specialised Skills | RTO 46344 | Version 2.0

Document details	
Purpose	This procedure sets out how Specialised Skills keeps personal information safe. It also says how people can see and correct their information, and what to do if there is a data breach.
Applies to	All the personal information that Specialised Skills holds, in any system or on paper.

Roles: both owners carry out all **Owner** steps. They are also the Privacy Officers.

STUDENT Yellow rows are the steps students (or other people) complete.

1. Where information is kept

System	What it holds	Who has access	Data location
Bookeo	Bookings, contact details, payments	Owners	North America and Europe
Vettrak	Enrolment, USI, AVETMISS data, results, certificates	Owners	Australia
Google Workspace (Drive, Gmail)	Assessment material files, LLND, forms, emails, registers (04 Students)	Owners	Around the world (Google data centres)
Payment provider (Stripe)	Card details (not seen or stored by Specialised Skills)	Provider only	United States
Accounting software (Xero)	Invoices, payments	Owners	United States (Amazon Web Services)
Paper	Assessments, sign-in sheets, consent forms	Owners, trainer	Scanned, then securely destroyed

2. Everyday protection

Do	Do not
• Use your own login, with multi-factor authentication (a code sent to your phone), for every system • Save copies of ID documents only in the student's file, where only the owners can see them • Lock phones and laptops with a passcode, and keep them updated • Share Drive folders with named owners only • Check the address before you send an email with personal information • Keep paper records in a locked box at training until they are scanned • Scan paper records to the student's file in Google Drive, then shred the paper copy • Look at ID documents and record only the type and number	• Share passwords or accounts • Use "anyone with the link" sharing • Keep student information in personal email, on USB drives or in personal cloud accounts • Leave paperwork in a vehicle or at a client site • Discuss a student's information with an employer without consent

3. Steps

Step	Who	What to do	Record
A. Seeing your information			
1	**STUDENT**	Email admin@specialisedskills.com.au to ask for a copy of your information. You can also see your results any time on your USI transcript at usi.gov.au.	Email
2	Owner	Check who is asking. The request must come from the email on file. The person also confirms their date of birth and address. If you are not sure, check their photo ID.	Access and Correction Log
3	Owner	Send the information within 30 days. It is free. Send it in a secure way. If you refuse any part, give the reasons and explain how to complain.	Access and Correction Log
B. Correcting your information			
4	**STUDENT**	Email admin@specialisedskills.com.au and say what needs to change. Send proof if it is needed, for example for a name change. Update your own details in the USI portal.	Email
5	Owner	Check who is asking. Correct the record in all systems within 10 business days. If the information went to another organisation, tell them if the person asks. If you refuse, give the reasons in writing. Add the person's own statement to the record.	Systems updated; log

Step	Who	What to do	Record
C. Requests from other people			
6	Owner	Employer or parent: only give information if the student agrees in writing, or agreed when they enrolled. ASQA, NCVER, the USI Registrar or SafeWork NSW: give what the law requires. Police or a court: only give information if they send a written legal request, such as a warrant or subpoena. Write down what you gave.	Access and Correction Log

4. Managing a data breach

A data breach is when personal information is lost, or when someone sees or shares it without permission. For example, an email goes to the wrong person, a phone or folder is lost, an account is hacked, or a Drive link is made public.

Step	Who	What to do	Record
7	Anyone	Tell an owner straight away. Do not delete evidence.	Phone or email
8	Owner	Stop it from spreading on the same day: • ask the person who got the email to delete it and confirm in writing • change passwords and sign out other sessions • wipe a lost device remotely, and remove public links.	Data Breach Register (Privacy Register)
9	Owner	Within 30 days at most, work out what information was involved and how many people it affects. Decide if serious harm is likely. For example, if ID numbers or USIs got out, someone could steal a person's identity.	Data Breach Register (Privacy Register)
10	Owner	If serious harm is likely, tell the people affected and the OAIC as soon as you can. Use the OAIC online form. Tell people what happened and what they should do. This is because Specialised Skills follows the Notifiable Data Breaches scheme.	OAIC form; letters
11	Owner	Tell others if you need to. Tell the police if there was a crime, the bank or provider if an account was hacked, and the USI Registrar if USIs were involved.	Data Breach Register (Privacy Register)
12	Owner	Find out why it happened and fix it. Write down what you did in the Continuous Improvement Register.	CI register

5. Keeping and destroying records

These times come from the Records Management Policy.

Record	Keep for	Then
Assessment evidence	2 years after the assessment decision	Securely delete or shred
Results and statements of attainment	30 years (Vettrak)	Transfer to ASQA if the RTO closes

Record	Keep for	Then
Enrolment forms, consent forms, LLND results and support records	7 years after the course	Securely delete or shred
Financial records	5 years	Securely delete or shred
Complaints, appeals, misconduct and data breach records	7 years	Securely delete or shred
Child safety incident records	45 years	Securely destroy
Information collected only for a USI application	Until the application is made	Destroy

Procedure information

Responsibility: The owners approve this procedure, are the Privacy Officers and make sure it is followed.

Related documents: Privacy Policy; Records Management Policy; Complaints and Appeals Procedure; Enrolment Procedure; Filing guide; Privacy Register (Data Breach Register and Access and Correction Log).

Requirements: Privacy Act 1988 (Australian Privacy Principles 1, 11, 12 and 13; Notifiable Data Breaches scheme); Student Identifiers Act 2014; Standards for RTOs 2025 (Compliance Standards).

Document control: Version 2.0, approved by Greg Cusack on 26 October 2026. New procedure. Next review: 18 October 2027.

Student summary

How students see or correct their information, and what happens if something goes wrong.

