Safe Skills
Safe Skills, Strong Teams

Information Security Policy

1. Purpose

Safe Skills Training Ltd protects information and systems to maintain confidentiality, integrity, and availability.

This policy sets minimum standards for:

- Secure handling of information
- Secure use of devices and accounts
- Access control
- Backups and retention
- Incident reporting and response

2. Scope

This policy applies to:

- All business information, in any format (digital, paper, verbal)
- All systems used for business purposes (email, cloud storage, websites, booking systems, CRM, accounting, forms, spreadsheets)
- All devices used for business purposes (company-owned or personally-owned)

This policy applies to:

- The Director/Lead Educator
- Employees (current or future)
- Associates and subcontractors

3. Principles

Safe Skills Training Ltd applies the following principles:

- Least privilege: access is limited to what is required for the role
- Need-to-know: information is shared only with those who require it
- Secure by default: security settings are enabled and maintained
- Accountability: access and actions are attributable to an individual
- Continuous improvement: security controls are reviewed and improved

4. Roles and responsibilities

4.1 Director/Lead Educator

The Director/Lead Educator is responsible for:

- Implementing and maintaining information security controls
- Managing user access and permissions
- Ensuring staff/associates understand and follow this policy
- Ensuring information security incidents are recorded and managed
- Ensuring suppliers and associates meet required security standards

4.2 Staff, associates, and subcontractors

Staff, associates, and subcontractors are responsible for:

- Following this policy and related procedures
- Protecting credentials and devices
- Reporting suspected or actual security incidents immediately

5. Information classification and handling

5.1 Information types

Safe Skills Training Ltd handles:

- Personal data (learners, clients, enquirers, staff/associates)
- Special category data where required for delivery or adjustments
- Business records (quotes, invoices, contracts, policies, QA records)
- Training materials (workbooks, slides, assessments, competency evidence)

5.2 Handling rules

- Personal data is collected and used only for defined business purposes.
- Special category data is collected only when required and kept to the minimum necessary.
- Information is stored only in approved systems.
- Information is not shared using personal messaging apps or personal email accounts.

6. Access control and authentication

6.1 Accounts

- Every user has their own account.

- Shared accounts are not used.
- Accounts are removed or disabled when access is no longer required.

6.2 Passwords and multi-factor authentication (MFA)

- Passwords are unique and not reused across systems.
- MFA is enabled on all systems that support it.
- Passwords are not shared or written where others can access them.

6.3 Permissions

- Access permissions are reviewed at least annually and when roles change.
- Access to learner records and assessment evidence is restricted.

7. Device security

7.1 Approved devices

Business information is accessed only on devices that:

- Are protected by a passcode/password
- Have automatic screen lock enabled
- Have up-to-date operating system and security updates

7.2 Anti-malware and security software

- Anti-malware protection is enabled where available.
- Devices are kept updated.

7.3 Storage and encryption

- Full-disk encryption is enabled where available.
- Removable media (USB drives) is not used for personal data unless encrypted.

7.4 Lost or stolen devices

Lost or stolen devices that may contain or access business information are reported immediately to the Director/Lead Educator.

8. Email and communications security

- Business email accounts are used for business communications.
- Emails containing personal data are sent only to verified recipients.
- Attachments containing personal data are minimised.
- Links to secure cloud files are used instead of sending sensitive attachments where possible.

9. Cloud storage and file management

9.1 Approved storage

Business files are stored in approved cloud storage with access control.

9.2 Folder and file permissions

- Access is granted to individuals and restricted to the minimum required.
- Links are not shared publicly unless the content is intended for public use.

9.3 File naming and version control

- Files use professional, clear names.
- Controlled documents use version numbers.

10. Backups and recovery

- Business-critical information is backed up using the cloud provider's controls and recovery features.
- Recovery is tested at least annually.

11. Secure working (including travel and venues)

- Devices are not left unattended in public.
- Screens are positioned to reduce shoulder-surfing.
- Paper records are kept secure and returned for secure storage.
- Public Wi-Fi is avoided for sensitive tasks.

12. Data retention and secure disposal

- Digital records are retained and disposed of in line with the Candidate Records Keeping Policy and Data Protection Policy.
- Paper records are shredded or securely destroyed.
- Devices are wiped before disposal or reuse.

13. Supplier and subcontractor security

Suppliers, associates, and subcontractors who handle business information must:

- Use secure accounts and devices
- Follow confidentiality requirements
- Report incidents immediately
- Use approved storage and communication methods

14. Information security incidents

14.1 What is an incident

An information security incident includes:

- Lost or stolen devices
- Unauthorised access to accounts or files
- Suspected phishing or credential compromise
- Accidental disclosure of personal data
- Malware infection
- System outages affecting availability of critical records

14.2 Reporting

Incidents are reported immediately to: **andy@safeskillstraining.com**

14.3 Response

Safe Skills Training Ltd:

- Secures accounts and systems
- Preserves evidence
- Assesses impact and risk
- Notifies affected parties and regulators where required under law
- Records actions and outcomes

15. Training and awareness

- All staff/associates receive an information security briefing before accessing business systems.
- Refresher briefings are completed at least annually.

16. Monitoring and review

- **Policy owner:** Director/Lead Educator
- **Review frequency:** Annually, or sooner if systems, risks, or legal requirements change

Version control

Version	Date	Summary of changes
1.0	19/04/2026	First issue

Safe Skills Training Ltd Website: https://www.safeskillstraining.com Email: andy@safeskillstraining.com Business phone: 0330 043 4663