

Information Security Policy

24th December 2025 - ST05

Version No	1
Date	29th December 2025
Approved	
Document Owner	
Contributors	
Date of Review	December 2026

Amendment Register

Date Amended	
Amendments	

1. Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information held by SENSational Tutors Limited, particularly sensitive information relating to children, parents, guardians, and tutors.

2. Scope

This policy applies to:

- All staff, tutors, and contractors
- All information processed by the company, whether:
 - Electronic or paper-based
 - Stored on company systems or personal devices
- All working locations, including home and remote settings

3. Information Covered

Information includes, but is not limited to:

- Client names, dates of birth, and contact details
- Educational records, assessments, lesson notes, and progress reports
- Special Educational Needs, health, and safeguarding information
- Parent/guardian contact details and billing information
- Tutor records and safeguarding documentation

4. Roles and Responsibilities

Management

- Overall responsibility for information security
- Ensure appropriate technical and organisational measures are in place
- Handle and report security incidents and data breaches

Staff and Tutors

- Follow this policy at all times
- Protect devices, passwords, and information
- Report any actual or suspected security incidents immediately

5. Access Control

- Access to information is granted **only on a need-to-know basis**
- Each user must have their own login credentials
- Passwords must:
 - Be strong and kept confidential
 - Not be shared with anyone
 - Be changed if there is any concern they are compromised
- Devices must be locked when unattended

6. Device and System Security

- All devices used for work purposes must:
 - Be protected by a password, PIN, or biometric lock
 - Have up-to-date operating systems and security updates
- Built-in security features (e.g. antivirus, firewall) must be enabled
- Lost or stolen devices must be reported immediately

7. Data Storage and Handling

Electronic Data

- Stored only on approved systems (e.g. secure cloud platforms)
- Sensitive files should be encrypted where possible
- Personal data must not be stored unnecessarily on personal devices

Paper Records

- Stored in locked cabinets or secure locations
- Access restricted to authorised individuals
- Not left unattended in shared or public spaces

8. Email and Communication

- Personal and sensitive information must be shared securely
- Emails must only be sent to verified recipients
- Extra care must be taken when:
 - Using email
 - Messaging apps
 - Video conferencing platforms
- Sensitive information must not be shared via informal or unsecured channels

9. Data Minimisation and Retention

- Only information necessary for tutoring, safeguarding, and legal obligations is collected
- Information is retained only for as long as required
- Data is securely deleted or destroyed when no longer needed

10. Remote Working and BYOD (Bring Your Own Device)

Remote Working

- When working remotely, individuals must:
 - Ensure screens are not visible to others
 - Avoid discussing sensitive information where they may be overheard
 - Log out of systems when work is complete

Bring Your Own Device (BYOD)

Where personal devices are used for work purposes:

- Devices must be:
 - Password- or PIN-protected
 - Set to lock automatically when not in use
- Work information must:
 - Be stored only on approved systems
 - Not be saved permanently to personal devices
- Devices must not be shared with family members or others
- Loss, theft, or compromise of a device must be reported immediately

11. Incident and Breach Management

A security incident includes:

- Loss or theft of a device
- Accidental sharing of information
- Unauthorised access to data
- Malware, phishing, or suspected hacking

All incidents must be reported **immediately** to management.

Appropriate action will be taken, including investigation, containment, and notification where required.

12. Training and Awareness

- All staff and tutors receive basic information security guidance
- Awareness is refreshed periodically or when risks change
- Individuals are encouraged to raise concerns or questions

13. Policy Review

This policy will be reviewed:

- At least annually
- Following any security incident
- When there are changes to law, technology, or business practices

14. Compliance

Failure to comply with this policy may result in:

- Disciplinary action
- Removal of system access
- Contractual consequences

Information Security – Do & Don't Guide For Tutors and Staff

Do:

- ✓ Lock your device when not in use
- ✓ Use strong, private passwords
- ✓ Check email recipients carefully before sending
- ✓ Store work files only on approved systems
- ✓ Keep paper records locked away
- ✓ Report mistakes or concerns immediately
- ✓ Be mindful of privacy when working from home

Don't:

- ✗ Share passwords or accounts
- ✗ Leave devices unattended in public places
- ✗ Store client information permanently on personal devices
- ✗ Send sensitive information via informal messaging apps
- ✗ Discuss clients where you can be overheard
- ✗ Ignore lost devices or accidental disclosures