



SENSES Learning Hub

ICT & Internet Acceptable Use Policy

Created: 11.09.26

Review date: 11.09.27

Dawn Oughtibridge (Director)

A handwritten signature in grey ink, appearing to read "Dawn", written over a light blue horizontal line.

John Fox (Director)

A handwritten signature in grey ink, appearing to read "John Fox", written over a light blue horizontal line.



1. Introduction and aims

Information and communications technology (ICT) is an important part of how SENSES Learning Hub operates. It supports teaching and learning, communication, administration and the safe and effective delivery of our provision.

ICT and internet use can also create risks relating to safeguarding, data protection, cyber security and online behaviour. This policy sets out clear and proportionate expectations for the use of SENSES ICT facilities and online services.

This policy aims to:

- Support safe and responsible use of ICT and the internet
- Protect young people, staff, self-employed practitioners, visitors and SENSES information
- Support our safeguarding, data protection and social media policies
- Reduce the risk of cyber attacks, data breaches and inappropriate online activity
- Help young people develop safe and appropriate digital skills

This policy applies to anyone using SENSES ICT facilities, including staff, Directors, self-employed practitioners, volunteers, young people and visitors.

Breaches may be managed under the relevant SENSES policy, agreement or contract.

2. Relevant legislation and guidance

This policy is informed by:

- Data Protection Act 2018 and UK GDPR
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- Education and Inspections Act 2006, where applicable
- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- Information Sharing to Safeguard Children and Young People statutory guidance 2026
- Alternative Provision statutory guidance
- Non-School Alternative Provision Voluntary National Standards
- National Cyber Security Centre guidance on cyber security
- UK Council for Internet Safety guidance relating to online safety and the sharing of nude and semi-nude images
- Department for Education guidance on filtering and monitoring and digital and technology standards, where relevant to our provision



SENSES is an independent alternative provision provider. Some DfE guidance applies specifically to schools and colleges rather than directly to independent AP providers. Where this is the case, SENSES uses the guidance as a framework for good practice where appropriate.

3. Definitions

ICT facilities means the computers, laptops, tablets, phones, software, internet services, networks, online platforms and other digital equipment or services used by SENSES.

Users means anyone authorised to use SENSES ICT facilities.

Personal use means use that is not directly related to work or the agreed purpose for which SENSES ICT facilities are being used.

4. Unacceptable use

The following are unacceptable when using SENSES ICT facilities or systems:

- Using ICT to bully, harass, threaten or discriminate against another person
- Accessing, creating, storing or sharing illegal, pornographic or seriously harmful material
- Sharing confidential or personal information without authorisation
- Attempting to gain unauthorised access to accounts, systems, files or data
- Sharing passwords or allowing others to use personal logins
- Installing unauthorised software or connecting unauthorised equipment to SENSES systems
- Deliberately damaging, disrupting or compromising SENSES ICT systems
- Using ICT to facilitate fraud, scams, phishing or other criminal activity
- Circumventing security, filtering or monitoring systems
- Using SENSES systems in a way that could place a young person or another person at risk
- Using ICT in a way that is racist, antisemitic, extremist or otherwise discriminatory
- Sharing images or information relating to young people without appropriate authorisation
- Any other activity that is unlawful or presents a significant safeguarding, data protection or cyber security risk

This is not an exhaustive list. The Directors will use professional judgement when dealing with other forms of inappropriate ICT use.

4.1 Exceptions

Where ICT use is required for a legitimate SENSES activity that might otherwise fall within this section, the Directors may authorise it.

4.2 Response to breaches



Concerns about ICT use will be dealt with proportionately and may involve the Directors, safeguarding procedures, the Staff Code of Conduct, Behaviour Policy, relevant contractual arrangements or other appropriate action.

5. Staff and self-employed practitioners

5.1 Access to SENSES ICT

The Directors manage access to SENSES systems, accounts, devices and information.

Users must:

- Only access information they are authorised to access
- Keep passwords and login details secure
- Use multi-factor authentication where available
- Report suspected breaches, lost devices or suspicious activity to the Directors promptly
- Take reasonable steps to keep devices used for SENSES work secure and up to date

5.2 Email, phones and communication

SENSES work should normally be conducted through agreed SENSES communication channels.

Self-employed practitioners may use their own professional devices and systems where this has been agreed with SENSES, provided that confidentiality, safeguarding and data protection requirements are maintained.

Staff and practitioners should not routinely provide young people with personal contact details or use personal communication channels for direct contact with young people unless this has been specifically agreed as part of their role and is appropriate and safe.

Work-related information must not be stored or shared in a way that could compromise the confidentiality or security of young people, families, staff or SENSES.

5.3 Personal ICT use

Reasonable personal use of SENSES ICT may be permitted where it does not interfere with work, compromise security or involve inappropriate material.

SENSES may restrict personal use where there is a safeguarding, data protection, cyber security or operational concern.

5.4 Personal social media

SENSES does not require staff, Directors or self-employed practitioners to hide their identity, change their name or use anonymous social media accounts. Individuals may use their own name



and identify themselves professionally, including identifying their connection with SENSES, if they choose to do so.

Everyone working with SENSES is expected to:

- Maintain appropriate professional boundaries with young people
- Never accept inappropriate contact or engage in inappropriate communication with a young person
- Never share confidential information about young people, families, colleagues or SENSES
- Never post photographs or videos of young people connected with SENSES without appropriate authorisation
- Avoid posting material that could reasonably undermine safeguarding, professional boundaries or trust in their role
- Consider the impact of publicly available content where it could directly affect their professional role

SENSES recognises that staff and self-employed practitioners have private lives and personal social media accounts. The purpose of this policy is not to control lawful personal activity but to protect young people, individuals and SENSES from inappropriate online conduct.

Where a young person attempts to contact a member of staff or practitioner through personal social media, the individual should maintain the appropriate professional boundary and inform the Directors where the contact is persistent, concerning or relevant to safeguarding.

5.5 SENSES social media accounts

The official SENSES social media accounts are managed by the Directors or other people specifically authorised by them.

Anyone authorised to contribute to SENSES social media must follow the SENSES Social Media Policy and appropriate data protection and safeguarding procedures.

5.6 Remote working

Anyone accessing SENSES information remotely must take reasonable steps to prevent unauthorised access.

SENSES information must not be left visible or accessible to other people and devices should be appropriately protected by passwords, PINs or equivalent security.

6. Young people

ICT and internet access is provided to young people as part of their learning and development.

Young people using SENSES ICT must:

- Follow staff guidance
- Use equipment appropriately

- Respect other people's privacy
- Not access or share inappropriate or harmful material
- Not attempt to access another person's account or information
- Not use ICT to bully, threaten or discriminate against another person
- Tell a member of staff if they encounter something online that makes them feel uncomfortable, worried or unsafe

ICT use will normally be supervised and appropriate filtering and other safeguarding measures will be used where available.

If a safeguarding concern arises from a young person's use of a device or online service, staff will follow SENSES safeguarding procedures and seek advice from the Directors or DSL.

7. Parents and carers

Parents and carers are not routinely provided with access to SENSES ICT systems.

Where a parent or carer is given access for a specific purpose, they are expected to respect confidentiality and use the access responsibly.

Parents and carers are encouraged to support young people in developing safe and respectful online behaviours.

8. Data security

SENSES will take reasonable and proportionate steps to protect its digital systems, devices and information.

Users are expected to:

- Use strong and secure passwords
- Use multi-factor authentication where available
- Keep devices and software updated
- Use appropriate security and anti-virus protection
- Lock devices when unattended
- Only access information they are authorised to access
- Report suspected data breaches or cyber security incidents promptly
- Avoid using unapproved storage or file-sharing services for SENSES information

Personal data must be handled in accordance with the SENSES Data Protection Policy and current data protection legislation, including the UK GDPR, Data Protection Act 2018 and relevant provisions of the Data (Use and Access) Act 2025.

SENSES will maintain appropriate backups of important organisational information.

9. Protection from cyber attacks



SENSES will take proportionate steps to reduce cyber security risks.

This includes:

- Using strong authentication and multi-factor authentication where available
- Keeping systems and software appropriately updated
- Maintaining appropriate backups
- Providing staff and practitioners with appropriate information about common cyber threats
- Taking reasonable steps to protect SENSES accounts and online services
- Reviewing access to SENSES systems when roles change or individuals cease working with SENSES
- Responding promptly to suspected cyber security incidents

All users have a role in protecting SENSES from cyber attacks. NCSC guidance emphasises the importance of securing accounts, devices, backups and online services, particularly for small organisations.

10. Internet access

SENSES provides secure WiFi for appropriate educational and work purposes.

10.1 Young people

Young people may access SENSES WiFi with staff permission and supervision.

Access to online services will be managed according to the activity, age and individual needs of the young person.

Where filtering or monitoring is available, it will be used proportionately to support online safety.

10.2 Staff, practitioners and visitors

Staff and self-employed practitioners may use SENSES WiFi for legitimate work purposes.

Visitors may only use SENSES WiFi where authorised.

The WiFi password must not be shared with unauthorised individuals.

11. Monitoring and review

SENSES may monitor the use of its ICT systems, accounts and network where this is necessary and proportionate for safeguarding, cyber security, data protection, operational or legal purposes.

Any monitoring will be carried out in accordance with applicable law and SENSES policies.



SENSES will maintain appropriate filtering and monitoring arrangements where required and proportionate to the risks within the provision.

12. Related policies

This policy should be read alongside:

- Data Protection Policy
- Safeguarding and Whistleblowing Policy
- Staff Code of Conduct
- Social Media Policy
- Behaviour Policy
- Online Safety arrangements
- Complaints Policy

The Directors will review this policy annually and sooner where there are significant changes to legislation, guidance, technology or the needs of SENSES

Appendix 3: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the provision will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

TERM	DEFINITION
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

—