



Acceptable Use Policy

Policy Reviewed by:	Hayley Richardson-Byrne / Suzy Hollett
Date:	01.09.2026
Policy Verified by:	Senior Management Team
Date:	06.10.2026
Date for Next Review:	01.09.2027

Key Personnel	
Proprietor	Sara Llewellyn
Designated Safeguarding Lead (DSL)	Suzy Hollett
Deputy Headteacher	Natalie Lovelock
HR Manager	Hayley Richardson-Byrne
Business Manager	Sophie Illingworth
IT Manager	Jamie Martin
Teaching Staff	Joe Ross Ryan Colvin

1. Policy Statement

Maple Haven School is a small independent specialist SEND school providing education for up to 14 pupils. The school recognises that technology plays a vital role in learning, communication, safeguarding, administration and professional practice. The school also recognises that the inappropriate use of technology can place pupils, staff and the wider school community at risk. This policy sets out the expectations for the safe, responsible and professional use of information and communication technology (ICT), electronic devices, internet services, social media and artificial intelligence (AI). The Proprietor, Sara Llewellyn, has overall responsibility for ensuring that appropriate systems and procedures are in place to promote online safety, cyber security, data protection and safeguarding throughout the school. All staff, volunteers, contractors, visitors and pupils are required to comply with this policy.

2. Purpose

The purpose of this policy is to:

- Promote safe and responsible use of technology.
- Safeguard children from online risks and harm.
- Protect pupils' personal information and privacy.
- Ensure compliance with data protection legislation.
- Prevent misuse of school equipment and systems.
- Support professional and ethical staff conduct.
- Maintain clear boundaries between staff and pupils.
- Protect the reputation of Maple Haven School.
- Ensure appropriate use of emerging technologies, including artificial intelligence.

3. Related Legislation and Guidance

This policy should be read alongside:

- Keeping Children Safe in Education 2026 (KCSIE)

- Working Together to Safeguard Children 2026
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Education Act 2002
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Prevent Duty Guidance
- Maple Haven School Child Protection and Safeguarding Policy
- Maple Haven School Online Safety Policy
- Maple Haven School Staff Code of Conduct
- Maple Haven School Data Protection Policy

4. Scope

This policy applies to:

- All employees.
- Volunteers.
- Agency staff.
- Consultants.
- Contractors.
- Visitors.
- Pupils.
- Anyone using school ICT systems or devices.

The policy applies whether technology is used:

- On school premises.
- During educational visits.
- During off-site activities.
- When working remotely.
- Through school-issued equipment.
- Through personal devices connected to school systems.

5. Roles and Responsibilities

Proprietor

Sara Llewellyn is responsible for:

- Ensuring effective ICT, safeguarding and online safety arrangements are in place.
- Monitoring compliance with this policy.
- Ensuring the school has appropriate cyber security measures.
- Ensuring suitable filtering and monitoring systems are operational.

- Investigating serious breaches of this policy.
- Overseeing disciplinary action where required.

Designated Safeguarding Lead (DSL)

Suzy Hollett is responsible for:

- Managing online safety concerns.
- Responding to safeguarding incidents involving technology.
- Recording and investigating concerns.
- Liaising with external agencies where necessary.
- Providing guidance and training for staff.
- Monitoring online safety risks affecting pupils.

Deputy Headteacher

Natalie Lovelock is responsible for:

- Supporting the implementation of this policy.
- Monitoring staff compliance.
- Promoting safe use of technology across the school.
- Supporting online safety education for pupils.

IT Manager

Jamie Martin (IT Manager) is responsible for:

- Maintaining the school's ICT infrastructure and network security.
- Ensuring appropriate filtering and monitoring systems are operational and effective.
- Supporting the implementation of cyber security measures.
- Managing user accounts, passwords and access permissions.
- Monitoring and responding to technical security incidents.
- Maintaining secure backup and recovery arrangements.
- Providing technical advice on online safety and cyber security.
- Supporting staff training in the safe use of technology.
- Working closely with the DSL, Suzy Hollett, regarding online safety incidents and safeguarding concerns involving technology.
- Reporting significant ICT risks and cyber security concerns to the Proprietor, Sara Llewellyn.

Business Manager

Sophie Illingworth (Business Manager) is responsible for:

- Supporting the procurement and management of ICT resources.
- Assisting with compliance relating to data protection and information governance.

- Ensuring appropriate records are maintained in relation to ICT assets and devices.
- Supporting cyber security and business continuity planning.
- Monitoring expenditure relating to ICT systems and services.
- Supporting investigations into data breaches or misuse of school technology where appropriate.
- Working with the Proprietor and IT Manager to ensure technology resources remain suitable, secure and effective.

HR Manager

Hayley Richardson-Byrne is responsible for:

- Including this policy within staff induction processes.
- Supporting investigations relating to employee conduct.
- Maintaining records relating to policy breaches.
- Supporting disciplinary procedures where required.

Teaching Staff

Teaching staff, including Joe Ross and Ryan Colvin, are responsible for:

- Modelling safe and responsible use of technology.
- Supervising pupils when using digital devices and online resources.
- Promoting online safety as part of everyday teaching.
- Reporting any online safety, safeguarding or cyber security concerns immediately.
- Following all requirements of this policy and associated safeguarding procedures.
- Supporting pupils to understand how to stay safe online and use technology appropriately.
- Using school systems professionally and securely.

Staff

All staff are responsible for:

- Following this policy at all times.
- Protecting confidential information.
- Reporting concerns immediately.
- Maintaining professional boundaries online.
- Ensuring technology is used safely and appropriately.

6. Use of School ICT Systems

The school's ICT systems are provided to support education, safeguarding and business operations.

Users must:

- Use school equipment appropriately.
- Follow all safeguarding requirements.
- Access only authorised systems.
- Maintain confidentiality.
- Protect usernames and passwords.
- Use technology in a professional manner.
- Report faults, breaches or concerns promptly.

Users must not:

- Attempt to bypass security systems.
- Access inappropriate material.
- Download unauthorised software.
- Use systems for illegal purposes.
- Introduce malware or malicious software.
- Use systems in a way that could damage school networks.
- Share passwords.
- Access another person's account.

7. Internet Use

Internet access is provided to support learning and professional responsibilities.

All users must:

- Access only appropriate websites and online resources.
- Follow safeguarding expectations.
- Respect copyright and intellectual property laws.
- Ensure information obtained online is appropriate and reliable.

The following are strictly prohibited:

- Accessing extremist, harmful, offensive or illegal material.
- Gambling.
- Viewing or sharing offensive content.
- Uploading inappropriate images or videos.
- Participating in online activity that could bring the school into disrepute.
- Anonymous messaging designed to harass or intimidate others.

8. Email Use

School email accounts must be used professionally and responsibly.

Users must:

- Communicate respectfully.
- Consider confidentiality before sending information.

- Check recipients carefully before sending emails.
- Immediately report suspicious messages.

Users must not:

- Forward chain emails.
- Send offensive messages.
- Share confidential information without authorisation.
- Use school email for commercial purposes.

Email communications should always reflect the professional standards expected of staff at Maple Haven School.

9. Mobile Phones and Personal Devices

Maple Haven School recognises that staff may need to bring mobile phones onto site.

Given the vulnerability of pupils attending the school, strict controls are required.

Staff must:

- Store personal mobile phones in designated staff areas or lockers during teaching and direct pupil contact time.
- Keep mobile phones on silent.
- Use personal devices only during authorised breaks unless permission has been granted by the Proprietor or Deputy Headteacher.
- Ensure personal devices do not contain illegal or inappropriate material.

Staff must not:

- Use personal mobile phones when supervising pupils.
- Photograph or record pupils using personal devices.
- Share personal contact details with pupils.
- Use personal messaging applications to communicate with pupils.

Any concerns relating to mobile phone use must be reported immediately to the DSL, Suzy Hollett, and the Proprietor, Sara Llewellyn.

10. Photography and Video Recording

Photographs and videos may only be taken using authorised school equipment. Photographs may only be used for legitimate educational, safeguarding or promotional purposes approved by the school.

Staff must:

- Follow parental consent arrangements.
- Ensure images are appropriate and respectful.
- Store images securely.
- Transfer images to approved storage systems promptly.
- Delete images from devices once transferred.

Staff must never:

- Use personal devices to photograph pupils.
- Store pupil images on personal equipment.
- Share pupil photographs without authorisation.

All photographs and recordings will be stored and retained in accordance with the school's

Data Protection Policy.

11. Artificial Intelligence (AI)

Maple Haven School recognises the growing use of artificial intelligence technologies within education. Only approved AI systems may be used.

Staff must:

- Review all AI-generated content before use.
- Verify accuracy and reliability.
- Ensure safeguarding standards are maintained.
- Exercise professional judgement at all times.

Staff must not:

- Input confidential pupil information into public AI systems.
- Upload personal data to unauthorised platforms.
- Use AI as a substitute for professional decision-making.
- Rely on AI-generated material without verification.

AI must not be used to make safeguarding decisions or assessments without professional oversight.

Pupils using AI tools must do so under appropriate supervision.

12. Social Media

Staff are expected to maintain professional conduct online at all times.

Staff must:

- Maintain professional boundaries.
- Protect the reputation of the school.
- Follow confidentiality requirements.

Staff must not:

- Accept social media friend requests from pupils.
- Communicate with pupils through personal accounts.
- Post confidential information.
- Share photographs of pupils without permission.
- Publish content that could undermine professional standards.

Any concerns regarding social media conduct must be reported to Suzy Hollett (DSL).

13. Cyber Security

Maple Haven School takes cyber security seriously.

All users must:

- Use strong passwords.
- Keep passwords confidential.
- Lock devices when unattended.
- Report suspicious emails immediately.
- Report data breaches without delay.
- Follow school security procedures.

Users must not:

- Share passwords.
- Disable security software.
- Install unauthorised applications.
- Open suspicious attachments.
- Circumvent security controls.

The Proprietor, Sara Llewellyn, has overall responsibility for ensuring appropriate cyber security measures remain effective.

14. Filtering and Monitoring

Maple Haven School operates filtering and monitoring systems designed to support safeguarding and protect users.

Users should be aware that:

- Internet activity may be monitored.
- School systems may be reviewed.
- Security alerts may be investigated.
- Safeguarding concerns arising from monitoring systems may result in further investigation.

The DSL, Suzy Hollett, will work with the Proprietor, Sara Llewellyn, to review concerns identified through filtering and monitoring arrangements.

15. Reporting Concerns

Any concerns relating to:

- Online safety.
- Cyber security.
- Inappropriate content.
- Data breaches.
- Social media.
- Mobile device use.
- Artificial intelligence.
- Safeguarding risks.

must be reported immediately to DSL: Suzy Hollett

Where concerns involve members of staff, the matter must also be reported to Proprietor: Sara Llewellyn

The school will take all reports seriously and will investigate promptly.

Where required, referrals may be made to:

- The Local Authority Designated Officer (LADO).
- Children's Social Care.
- Police.
- Other safeguarding agencies.

16. Breaches of the Policy

Failure to comply with this policy may result in:

- Restricted access to school systems.
- Additional supervision or monitoring.
- Withdrawal of ICT privileges.
- Formal disciplinary action.
- Referral to external agencies.
- Dismissal where serious misconduct is identified.
- Criminal investigation where legislation has been breached.

Serious breaches will be reviewed by the Proprietor, Sara Llewellyn, with support from Suzy Hollett (DSL), Natalie Lovelock (Deputy Headteacher) and Hayley Richardson-Byrne (HR Manager), as appropriate.

17. Monitoring and Review

This policy will be reviewed annually or sooner where:

- Legislation changes.
- National guidance changes.
- A significant incident occurs.
- School practice requires amendment.