

St Nicholas School

Acceptable Use of Technology Statement



St. Nicholas School Canterbury

Policy Created	May 2026
Reviewing body	N/A - Emma Blackmore on behalf of Board of Governors
SLT responsibility	David Jenner
Review Date	19/5/2026
Date of Next Review	May 2027

St Nicholas School provides access to digital technology including networks, devices, internet services and cloud systems to support teaching, learning, communication and school administration. This Acceptable Use Policy ensures all users use technology safely, protect school systems and safeguard pupils and staff in line with UK GDPR and safeguarding legislation.

These expectations apply to all members of the school community including:

- Staff
- Pupils
- Governors
- Volunteers
- Visitors
- Parents accessing school systems

Use of school systems indicates acceptance of this policy.

General Expectations

All users must:

- use technology responsibly and safely
- protect confidential information
- follow safeguarding procedures
- comply with this policy and the Online Safety Policy.

Users must not:

- access illegal or inappropriate material
- engage in cyberbullying or harassment
- misuse school equipment or networks
- share confidential information.

Professional Conduct (Staff)

Staff must maintain professional standards when using digital technology.

Staff must use school systems for professional communication and must not communicate with pupils through personal email, social media or personal devices.

Confidential school information must not be shared online.

Artificial Intelligence (AI)

AI tools may only be used if approved by the school.

Users must not enter confidential information into AI systems and must check the accuracy of AI-generated information.

AI must support, not replace, professional judgement.

Cyber Security

Users must:

- create strong passwords
- keep passwords confidential
- lock screens when leaving devices
- report suspicious emails or links.

School systems are protected through antivirus software, secure cloud systems and monitoring tools.

School Devices

School devices are provided for educational or professional use.

Users must not install unauthorised software or share login details.

School data must only be stored on approved secure systems such as Microsoft 365.

Personal Devices

Personal devices may only be used in accordance with the school BYOD policy.

Personal devices must not store confidential school information or be used to photograph pupils unless authorised.

Mobile Phones

Staff must not use personal phones to contact pupils or parents about school matters.

Photographs of pupils must only be taken using school devices in line with the image use policy.

Social Media

Staff must maintain professional boundaries online.

Staff must not accept pupils as social media contacts or share school information online without permission.

Monitoring

The school operates filtering and monitoring systems that comply with DfE standards.

Internet activity, email and use of school devices may be monitored in accordance with safeguarding and data protection legislation.

Safeguarding

Any misuse of technology or safeguarding concern must be reported immediately to the Designated Safeguarding Lead. This includes cyberbullying, inappropriate contact or harmful online content.

We operate a 'screen lock' policy (when away from desk), to avoid any accidental data breach / confidentiality violation.

Misuse

Misuse of school systems may result in loss of access, disciplinary action or referral to external agencies including the police where necessary.

Agreement

All users must confirm that they understand and agree to follow this policy.

Full Name _____ sig. _____

Role (staff / student / visitor) _____ Date _____

Parents signature (if approp.) _____ Date _____

Access granted by _____ Date _____

This policy statement is part of the school Internet Safety Policy. It complies with the Kent e-Safety policy and is to be made available to all who have access to school computers or have use of the school network and / or internet systems.