St Nicholas School

Online Safety Policy

St. Nicholas School Canterbury

Policy Created	**January 2026**
Governing Body Committee	**FGB**
SLT responsibility	**David Jenner**
Date Reviewed by Governing Board	**20/3/26**
Date of Next Review	**September 2027**

ONLINE SAFETY POLICY (INC. GUIDANCE ON THE USE OF SOCIAL AND DIGITAL MEDIA)

1. Introduction

St Nicholas School recognises that digital technology is an essential part of modern life and education.

While technology provides significant opportunities for learning, communication and independence, it also presents risks that must be managed effectively.
Online safety is therefore recognised as a key element of safeguarding and child protection and is embedded throughout the school's safeguarding procedures.
This policy outlines how the school protects pupils, staff and the wider community when using digital technology and how the school promotes responsible and safe online behaviour.

Pupils with SEND may be at increased risk online due to communication needs, cognitive differences and social vulnerability. This can include increased susceptibility to grooming, coercion, misinterpretation of online content and difficulty recognising risk. Online safety approaches are therefore highly personalised and supported.

2. Scope of the Policy

This policy applies to all members of the school community including:
- Pupils
- Staff
- Governors
- Volunteers
- Visitors
- Parents and carers

It applies to the use of:
- School digital systems and devices
- Personal devices used on the school site
- Online behaviour outside school where it impacts the school community.

3. Legislative Framework

This policy reflects statutory guidance including:
- Keeping Children Safe in Education
- The Prevent Duty
- DfE Filtering and Monitoring Standards
- UK GDPR and the Data Protection Act 2018
- Searching, Screening and Confiscation Guidance
- UKCIS guidance on sharing nudes and semi-nudes

Online risks can be grouped into four categories:
Content – exposure to harmful or inappropriate material
Contact – harmful interaction with others online
Conduct – behaviour that increases risk of harm
Commerce – financial risks such as scams or gambling

4. Roles and Responsibilities

Governors

The governing body approves this policy and ensures appropriate filtering, monitoring and safeguarding arrangements are in place.

Headteacher and Senior Leadership Team

Senior leaders promote a culture of online safety and ensure staff training, filtering systems and safeguarding procedures are effective.

Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety, managing incidents, liaising with agencies and ensuring concerns are recorded and addressed.

Online Safety Lead

Supports the DSL in coordinating education, analysing trends and reviewing policy and procedures.

Staff

All staff must follow the Acceptable Use Policy, model responsible behaviour online, embed online safety in teaching and report concerns immediately.

Pupils

Pupils are expected to use technology responsibly, respect others online and report concerns to a trusted adult in line with their communication and understanding.

Parents and Carers

Parents are encouraged to reinforce safe online behaviour at home and support school expectations.

5. Online Safety Education

Online safety education is embedded across the curriculum through Computing, PSHE, assemblies and targeted interventions. The school recognises that pupils may be particularly vulnerable online due to SEND, mental health needs, communication difficulties or social circumstances.

The school teaches pupils how to:

- use technology safely and responsibly
- recognise online risks
- protect personal information
- report concerns.

Education is adapted to meet the needs of pupils with SEND and additional vulnerabilities.

6. Filtering and Monitoring

The school uses filtering and monitoring systems that meet the Department for Education Filtering and Monitoring Standards. Systems include network filtering, firewall protection and

monitoring software which identify potentially harmful searches or activity.
Filtering and monitoring systems are reviewed annually by the DSL, technical staff and senior leadership team with oversight from the governing body.

Filtering and monitoring systems support safeguarding but cannot replace effective staff supervision, professional curiosity and high-quality online safety education. Levels of supervision and access are determined by pupils' age, ability and individual risk assessment, with higher levels of direct supervision for more vulnerable learners. Some learners may require supervision and access to be reviewed regularly and agreed with the school's senior leadership team.

7. Cyber Security

The school takes appropriate steps to protect digital systems including:
- strong password policies
- secure cloud storage
- encrypted devices
- antivirus and malware protection
- regular system updates
- staff awareness training regarding phishing and cyber threats.

All new digital tools, apps or platforms are subject to risk assessment prior to use, particularly where they involve communication, data storage or online interaction.

8. Artificial Intelligence (AI) (Please refer to AI use appendix)

Artificial Intelligence tools are increasingly used in education. Staff may only use AI systems that have been approved by the school.
Staff must not enter personal or confidential information about pupils, staff or families into AI systems. AI tools must support professional judgement and must not replace safeguarding decisions or professional responsibility.

9. Social Media

Members of the school community must use social media responsibly.
Staff must not:
- communicate with pupils via personal social media accounts
- share confidential school information
- publish images of pupils without consent.

Official school social media accounts are managed by authorised staff and monitored appropriately.

10. Mobile Phones and Personal Devices

The use of personal devices is managed to reduce safeguarding risks.
Key expectations include:
- pupils who bring phones to school are expected to hand them in to class staff for the duration of the school day. They will be stored securely for the duration of the school day
- pupils must not use phones during lessons unless authorised

• staff must not use personal devices to contact pupils
• photographs of pupils must only be taken using school equipment.

11. Responding to Online Safety Incidents

All members of the school community are expected to report concerns, and pupils are explicitly taught how to do so in ways appropriate to their cognition and communication needs.

All members of the school community must report online safety concerns immediately to a DSL or Online Safety Lead. All records must be made using the CPOMS system.
Incidents will be recorded and investigated in line with safeguarding procedures.
Where appropriate, the school will involve external agencies including children's services, the police or CEOP.

12. Specific Safeguarding Concerns

The school has procedures for responding to:
• cyberbullying
• sharing nudes or semi-nudes
• online grooming or exploitation
• exposure to indecent images
• online radicalisation or extremism.
All such concerns are treated as safeguarding matters.

11. ONLINE SAFETY FOR STAFF AND PUPILS HOW WILL THE POLICY BE INTRODUCED TO PUPILS?

- Rules for Internet access will be posted in all rooms where computers are used.
- Pupils will be informed that internet and network use will be monitored
- An Online Safety training programme is established across the school to raise the awareness and importance of safe and responsible Internet use. The training should precede individual Internet access.
- The policy will be discussed at school council meetings, as part of the AIU policy statement review (see appendix A).
- The policy will be shared via PSHE, ICT and discreet Online Safety lessons (see scheme of work).

HOW WILL STAFF BE CONSULTED?

- All staff must accept terms of the 'Acceptable Internet and Equipment Use' statement before using any internet resource in school.
- All staff including teachers, supply teachers, supply staff, classroom assistants and support staff, will be provided with the Online Safety Policy, and its importance explained via the induction pack and training session, when joining the school. Updates to this policy will be delivered by explicit Online Safety training (an annual option), at teachers' meetings and / or via the whole-school Staff Training Meeting, once per year.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user by the Network Manager. Discretion and professional conduct is essential. Any such

monitoring will be conducted by the Senior Management Team.

HOW WILL PARENTAL SUPPORT BE ENLISTED?

The school works in partnership with parents and carers to promote online safety, including providing guidance and support for safe use at home.

- Parents' attention will be drawn to the School Internet Policy in newsletters, the Acceptable Internet and Equipment Use statement, the school prospectus and via the school Website. A copy of this policy and the 'Acceptable Use of Internet and Equipment Statement' will be provided to all new parents on admission to the school. Also provided at this time will be the permission for pupils to be included in photographs, videos and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This may include demonstrations, practical sessions and suggestions for safe Internet use at home.

EQUALITY, SAFEGUARDING AND EQUAL OPPORTUNITIES STATEMENT

St Nicholas School, in all policies and procedures, will promote equality of opportunity for students and staff from all social, cultural and economic backgrounds and ensure freedom from discrimination on the basis of membership of any group including gender, sexual orientation, family circumstances, ethnic or national origin, disability (physical or mental), religious or political beliefs.

As part of our commitment to meet the Public Sector Equality Duty (PSED), St Nicholas School aims to:

- Provide equal opportunity for all;
- Foster good relations, and create effective partnership with all sections of the community;
- Only take actions which does not discriminate unlawfully in service delivery, commissioning and employment;
- Provide an environment free from fear and discrimination, where diversity, respect and dignity are valued.

All aspects of Safeguarding will be embedded into the life of the School and be adhered to and be the responsibility of all staff will be embedded into the life of the school and be adhered to and be the responsibility of all staff.

Appendix E - Schools Online Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for Online Safety policy. Staff that contribute to the audit include: Designated Child Protection Coordinator, SENCO, Online Safety Coordinator, Network Manager and / or Head Teacher.

Does the school have an Online Safety Policy that complies with Kent guidance?		Y/N
Date of latest update:	Date of future review:	
The school Online Safety policy was agreed by governors on:		
The policy is available for staff to access at:		
The policy is available for parents/carers to access at:		
The responsible member of the Senior Leadership Team is:		
The governor responsible for Online Safety is:		
The Designated Safeguarding Lead is:		
The Online Safety Coordinator is:		
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school Online Safety Policy?		Y/N
Has up-to-date Online Safety training been provided for all members of staff? (not just teaching staff)		Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?		Y/N
Are all staff made aware of the schools expectation around safe and professional online behaviour?		Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an Online Safety incident of concern?		Y/N
Have Online Safety materials from CEOP, Childnet and UKCCIS etc. been obtained?		Y/N
Is Online Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?		Y/N
Are Online Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?		Y/N
Do parents/carers or pupils sign an Acceptable Use Policy?		Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?		Y/N
Has an ICT security audit been initiated by SLT?		Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?		Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?		Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?		Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?		Y/N
Does the school log and record all Online Safety incidents, including any action taken?		Y/N
Are the Governing Body and SLT monitoring and evaluating the school Online Safety policy and ethos on a regular basis?		

Appendix F - Online Safety Contacts and References

Kent Support and Guidance
Kent County Councils Education Safeguards Team:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
Kent Online Safety Support for Education Settings

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police: www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101
Kent Public Service Network (KPSN): www.kpsn.net
Kent Safeguarding Children Board (KSCB): www.kscb.org.uk
Kent e–Safety Blog: www.kentesafety.wordpress.com
EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources
Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF):
www.iwf.org.uk **Lucy Faithfull Foundation:**
www.lucyfaithfull.org **Know the Net:**
www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk **NSPCC:** www.nspcc.org.uk/onlinesafety
Professional Online Safety Helpline:
www.saferinternet.org.uk/about/helpline **The Marie Collins Foundation:** http://www.mariecollinsfoundation.org.uk/ **Think U Know**: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/