TONBRIDGE
GRAMMAR SCHOOL

ONLINE SAFETY POLICY

Related Policies

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Data Protection Policy
- Electronic Information and Communications Systems Policy
- Staff Acceptable Use of ICT Policy
- Social Media Policy
- Academic Honesty Policy
- Behaviour Policy
- Anti-Bullying Policy
- Search and Confiscation Policy
- Use of Student Images Policy
- Mobile Phone Charter
- Privacy Notice
- Live Communications and Remote Education Protocols

Introduction

Online safety is an integral part of safeguarding at Tonbridge Grammar School. It encompasses the safe and responsible use of digital technologies, including the internet, social media, online communication platforms, mobile devices, wearable technology and emerging technologies such as generative artificial intelligence (AI).

This policy should be read alongside *Keeping Children Safe in Education (KCSIE)*, the School's Child Protection and Safeguarding Policy and all related safeguarding, behaviour, data protection and acceptable use policies.

The School recognises that technology plays a vital role in education and daily life. Students must therefore be equipped not only to use technology safely, but also to evaluate information critically, manage risks appropriately, act responsibly online and know how and when to seek support.

Online safety risks are commonly grouped into four categories:

- **Content** - exposure to harmful, illegal or inappropriate content.
- **Contact** - harmful interaction with others online.
- **Conduct** - behaviour which causes or increases the risk of harm.
- **Commerce** - risks associated with fraud, scams, gambling and financial exploitation.

The School adopts a whole school approach to online safety involving students, staff, trustees and parents.

Leadership and Responsibilities

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety, including understanding the filtering and monitoring systems and processes in place. The DSL works closely with technical staff, pastoral and senior leaders to ensure safeguarding arrangements remain effective and responsive to emerging risks.

The Board of Trustees receives regular reports regarding online safety, safeguarding trends, filtering and monitoring arrangements and their effectiveness. Trustees provide strategic oversight and challenge in relation to the School's online safety arrangements.

Online safety arrangements are reviewed regularly through:

- safeguarding records;
- filtering and monitoring reports;
- staff reporting;
- national and local safeguarding updates.

All members of the school community share responsibility for promoting safe, responsible and respectful online behaviour.

All staff are responsible for remaining vigilant to online safeguarding concerns and must report concerns, no matter how small, to the DSL in accordance with safeguarding procedures.
https://tonbridgegrammarschool.sharepoint.com/sites/StrategyGroup/_layouts/15/Do

c.aspx?sourcedoc={6F78C2B6-4B63-4FC5-B41F-52E1DC12D89B}&file=LGfL Online Safety Policy Template July 2026.docx&action=default&mobileredirect=true

Online Safety Education

An online safety education programme is established across the School to raise awareness of safe, responsible and respectful use of technology.

This is delivered through:

- PSHE lessons;
- assemblies and awareness events, including Safer Internet Day;
- Computing lessons;
- subject-specific curriculum opportunities;
- pastoral and safeguarding interventions where appropriate.

Students are taught to:

- evaluate online information critically;
- recognise misinformation, disinformation and conspiracy theories;
- understand online relationships and digital citizenship;
- recognise scams, phishing and online fraud;
- understand the benefits and risks of social media;
- respond appropriately to cyberbullying;
- understand the opportunities and dangers associated with AI-generated content;
- manage their digital footprint and online reputation;
- report concerns promptly and seek support when required.

The School also provides online safety information and guidance for parents and carers through communications, information evenings, newsletters and the School website.

Staff receive regular training to ensure they remain aware of current online safety risks, safeguarding developments and appropriate professional practice.

Acceptable Use

To protect all members of the school community, the School operates Acceptable Use Policies for students, staff and visitors.

All users are required to read and comply with the relevant Acceptable Use Policy before accessing School systems or devices.

Users are made aware that use of School networks, devices and platforms may be monitored for safeguarding, security and operational purposes.

Risk Assessment

The School takes all reasonable precautions to ensure that users access only appropriate material.

Emerging technologies, applications and platforms will be evaluated before use within the School. Where appropriate, risk assessments will consider:

- safeguarding implications;
- data protection requirements;
- educational value;
- age appropriateness;
- technical security arrangements.

Internet Use

The internet is an essential educational resource and an integral part of learning and administration within the School.

Students are taught to:

- use online resources responsibly;
- acknowledge information sources appropriately;
- respect copyright and intellectual property rights;
- evaluate information critically;
- validate information before accepting its accuracy.

Staff should guide students towards online activities that support planned learning outcomes and are appropriate for their age and understanding.

The Academic Integrity Policy provides additional guidance regarding the responsible use of online information and digital resources.

Filtering and Monitoring

The School operates age-appropriate filtering and monitoring systems designed to protect students from harmful or inappropriate content while supporting teaching and learning.

The School's filtering and monitoring arrangements are designed to meet the Department for Education Filtering and Monitoring Standards. The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place and works closely with technical staff to review their effectiveness regularly.

Filtering and monitoring arrangements are reviewed regularly by safeguarding and technical staff to ensure they remain effective and proportionate. Proposed changes are risk assessed before implementation.

Staff are expected to report:

- inappropriate content that bypasses filtering controls;
- overblocking that adversely affects learning;
- attempts to bypass security controls;
- concerns identified through monitoring systems.

The DSL reviews relevant filtering and monitoring information and ensures appropriate safeguarding action is taken where necessary.

Any material believed to be illegal will be reported to the appropriate authorities.

Data Protection and Cyber Security

The School recognises the close relationship between safeguarding, data protection and cyber security.

All members of the school community must comply with the School's Data Protection Policy, Cyber Security arrangements and Acceptable Use Policies.

Personal information must be handled securely and shared only where appropriate and lawful. Data protection legislation does not prevent the sharing of information where necessary to safeguard and promote the welfare of children.

The School maintains appropriate technical and organisational security measures to protect School systems, personal information and educational data.

Staff receive guidance and training regarding cyber security, phishing, password management and the safe handling of information.

Email and Messaging Systems

Students may only use approved School communication systems for educational purposes.

Students must immediately report any message they find alarming, distressing or inappropriate to a member of staff.

Students must not reveal personal information about themselves or others online or arrange to meet anyone known only through online communication.

Staff must only use School provided communication systems when communicating with students or parents.

Personal email accounts, social media accounts or messaging applications must not be used for professional communication with students.

Use of Generative Artificial Intelligence

The School recognises that generative artificial intelligence tools such as Microsoft Copilot, ChatGPT, Gemini and similar technologies are becoming increasingly common in education and society.

The School's approach is based on the principles of safety, transparency, educational value and academic integrity.

Staff and students must:

- use AI tools responsibly and critically;
- only use AI services approved through the School's IT, safeguarding and data protection processes;
- verify the accuracy of AI-generated content before relying upon it;
- acknowledge the use of AI where required by teachers or assessment regulations.

Personal data, safeguarding information, confidential School information and examination material must not be entered into AI systems unless specifically authorised and legally compliant.

Students will be taught about:

- misinformation and fabricated content;
- bias and inaccuracies;
- deepfakes and manipulated imagery;
- privacy risks;
- scams and fraud;
- ethical issues relating to AI.

The School recognises emerging safeguarding risks associated with generative AI, including deepfakes, manipulated imagery, AI-generated sexual content, misinformation, scams and harmful chatbot interactions. These topics will be addressed through safeguarding education, staff training and ongoing review of School procedures.

Use of AI in a way that breaches the Academic Integrity Policy may result in sanctions in accordance with School procedures.

Published Content

The School's website and online communications will contain the School's contact details but will not publish personal contact information relating to staff or students.

The Head Teacher retains overall responsibility for content published on behalf of the School and ensures published material is accurate, appropriate and compliant with legal requirements.

The School website and public communications will respect copyright, privacy and data protection requirements.

Student Images and Media

The School respects permissions granted by students, parents and carers regarding the use of photographs and video recordings.

The School will process images of students in accordance with data protection legislation and published consent arrangements.

The School recognises emerging risks associated with image manipulation technologies, including AI-generated and AI-altered imagery. When selecting images for publication, consideration will be given to privacy, safeguarding and the potential misuse of digital content.

Students' full names will not be published alongside photographs in publicly accessible online locations.

All staff must ensure photographs and videos are captured, stored, shared and deleted in accordance with School procedures and data protection requirements.

Parents and carers are expected to respect the privacy of other students and families when taking photographs or videos at School events.

Social Media

The School acknowledges that social media forms an important part of modern life.

All members of the school community are expected to communicate in a manner that is:

Kind, Necessary and Helpful.

The School expects students, staff, parents and visitors to behave online in ways consistent with the values and standards expected within the school.

Staff must maintain professional boundaries online and comply with the Staff Code of Conduct and Social Media Policy.

Staff must not communicate with students through personal social media accounts.

Students must not use social media in ways that constitute bullying, harassment, discrimination or behaviour that may bring harm to themselves or others.

Online Learning Platforms

The School uses online platforms including Microsoft 365 and other approved educational applications to support learning and communication.

Access to online learning platforms is restricted to authorised users.

Users must only upload material that is lawful, appropriate and compliant with copyright requirements.

Access will be removed when staff or students leave the School.

Sharing Nude and Semi-Nude Images

The School will respond to incidents involving the creation, possession or sharing of nude or semi-nude images in accordance with current national safeguarding guidance.

Where concerns arise:

- staff must not view, copy, print, save, share or delete images;
- staff must not request that images are shown to them;
- concerns must be reported immediately to the DSL;
- the DSL will determine appropriate next steps and whether external agencies should be involved.

The School seeks to balance effective safeguarding with a supportive approach that avoids unnecessary criminalisation of young people.

Responding to Incidents of Concern

All online safety concerns are safeguarding concerns and will be managed in accordance with the Child Protection and Safeguarding Policy.

Any member of the School community who becomes aware of an online safety concern must report it immediately using the School's safeguarding procedures.

Concerns relating to child sexual abuse, including abuse facilitated online, must be reported immediately to the DSL and managed in accordance with current safeguarding legislation and statutory guidance.

Particular attention should be given to concerns involving:

- child sexual abuse or exploitation;
- online grooming;
- harmful sexual behaviour;
- cyberbullying;
- extremist content;
- sharing of nude or semi-nude images;
- AI-generated sexual imagery;
- scams or financial exploitation.

Where necessary, the School will work with external agencies, including the Local Authority, Kent Safeguarding Children Partnership and Police.

All incidents will be recorded and reviewed to identify lessons learned and any changes required to School practice.

Use of Personal Devices

Tonbridge Grammar School operates a phone-free school day. The School believes that reducing access to mobile phones during the school day supports learning, wellbeing, positive social interaction and safeguarding.

Student Mobile Phones

Students may bring a mobile phone to and from School for safety and travel purposes. However, mobile phones must be switched off and stored in accordance with the School's Mobile Phone Charter throughout the school day.

Students must not access mobile phones or other personal communication devices during the School day except where authorised by a member of staff for a specific educational, safeguarding or medical purpose.

Where a student needs to contact a parent or carer during the school day, this should be arranged through the School Office. Likewise, parents and carers should contact the School Office if they need to pass an urgent message to a student.

Any breach of the Mobile Phone Charter may result in confiscation and sanctions in accordance with the Behaviour Policy.

Wearable Technology and Recording Devices

Personal recording devices, including smart glasses, body-worn cameras and similar wearable technology, must not be used on school premises without explicit permission.

Students must not:

- make audio recordings of staff or other students;
- make video recordings of staff or other students;
- photograph staff or other students without consent;
- use any device to record lessons, conversations or School activities unless explicitly authorised.

Unauthorised recording of any member of the school community may be treated as a safeguarding and/or disciplinary matter.

Staff Devices

Staff should keep personal mobile phones on silent mode during working hours and use them only in staff areas or for exceptional circumstances.

Staff and visitors must not use personal devices to:

- photograph students;
- record students;
- communicate with students in a professional capacity;
- store personal student information.

School-approved systems and school-issued devices must be used for all professional communication and recording activities.

Visitors, Contractors and Volunteers

Visitors, governors, contractors and volunteers must not use personal devices to photograph or record students unless specifically authorised by a member of the Senior Leadership Team.

Any authorised photography or recording must comply with safeguarding and data protection requirements.

School Devices

The School does not operate a bring-your-own-device scheme for teaching and learning. Only school managed devices may be used for teaching purposes.

Use of School devices must comply with all relevant School policies, including the Acceptable Use Policy, Data Protection Policy, Staff Code of Conduct and this Online Safety Policy.

All use of School networks, devices and platforms may be monitored for safeguarding, security and operational purposes.

Online Safety Priorities

The School identifies online safety priorities annually through safeguarding records, filtering and monitoring information, student voice, staff feedback and national guidance.

Current priorities include:

- responsible use of AI technologies;
- digital wellbeing and healthy technology use;
- online reputation and digital footprint;
- cyberbullying and harmful online interactions;
- misinformation and disinformation;
- image manipulation and deepfakes;
- online scams, fraud and financial exploitation.

The School's phone-free approach forms an important part of its wider commitment to online safety, digital wellbeing, positive relationships and healthy technology use.

These priorities are reviewed annually as part of the School's wider safeguarding arrangements.

Monitoring and Review

This policy will be reviewed annually by the Head Teacher and Designated Safeguarding Lead and updated sooner where necessary to reflect changes in legislation, statutory guidance, technology, safeguarding risks or School practice.

The School will continue to monitor developments in digital technology and online behaviour to ensure that its approach remains effective, proportionate and focused on the safety and wellbeing of students.

Policy Equality Statement

We have carefully considered and analysed the impact of this policy on equality and the possible implications for students with protected characteristics. This forms part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Approved: September 2026
Next review: September 2027
Policy owner: Head Teacher / Designated Safeguarding Lead