ONLINE SAFETY POLICY

Tonbridge School believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones, smart watches or games consoles. The internet and information communication technologies are an important part of everyday life and are an integral part of our teaching and learning strategies to access and deliver the curriculum, so boys must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Tonbridge School recognises it has a duty to provide our community with quality internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions. We recognise our clear duty to ensure that all boys and staff are protected from potential harm online.

This policy should be read in conjunction with the following School policies:

- Safeguarding Policy (Including the Child Protection Policy);
- Acceptable Use of Computers (Boys) Policy;
- IT Acceptable Use (Staff) Policy;
- Anti-Bullying Policy;
- Behaviour, Rewards and Sanctions Policy;
- The Cyberbullying Policy;
- Mobile Phone Use Policy;
- Emerging Technologies and Use of New Media Policy;
- Taking, Storing and Using Images of Pupils Policy;
- Guidelines for the Use of Email;
- Pastoral Education Policy;
- Relationship and Sex Education Policy;
- The Memoranda;
- The protocol for dealing with inappropriate and illegal material, within the Pastoral Handbook;
- The Prevent Duty at Tonbridge School;
- Staff Code of Conduct Policy.

The following measures are in place to support this policy:

- Regular Online Safety training for staff;
- The induction of new boys and staff;
- The Pastoral Education, Online Safety and ICT programmes;
- Guidance during any academic lesson about use of the internet to embed online safety education;
- Specific guidance to exam classes about plagiarism;
- Parents' Pastoral Evenings and the Parents' Pastoral Conference;
- The Anti-Bullying Coordinator(s) and the Anti-Bullying Council;
- Robust filtering and monitoring of boy activity across the network and internet;
- The Tonbridge Online Safety Council's publications and campaigns;
- Tutor Time.

AIMS OF THE POLICY

The aims of the Online-Safety Policy are:

- To promote the welfare and safeguarding of boys and staff at Tonbridge School;
- To ensure that boys are IT literate and can use the facilities to ensure that their educational provision is supported and enhanced;

- To promote responsible and effective use of electronic communication (including the use of the internet, social media and mobile phone technology).
- To educate boys and staff about the risks, responsibilities and potential criminal implications involved in the use of technology particularly those that fall under the four main areas of risk:
  - **content**: being exposed to illegal, inappropriate, or harmful content, for example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism;
  - **contact**: being subjected to harmful online interaction with other users; for example peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
  - **conduct**: online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (e.g., consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying;
  - **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- To raise awareness and counter instances of cyberbullying.
- To ensure that boys and staff know how to deal with any incidents of concern in relation to online safety.

SCOPE OF THE POLICY

This policy applies to all staff employed by the School (including teachers and support staff) and also Governors, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the School (collectively referred to as 'staff' in this policy) as well as to boys and their parents or carers. This policy applies to all access to the internet and use of information communication devices at the School, outside of the workplace including online which may have implications for the safeguarding of children, or during events or activities organised by the School, including personal devices, and also to occasions when boys, staff or other individuals have been provided with School issued devices for use off-site, such as work laptops, tablets or mobile phones.

MANAGEMENT OF THE POLICY

The Designated Safeguarding Lead (Mr C. J. C. Swainson) will serve as the Online-Safety Officer. Our Online-Safety Policy has been written by the School and draws on both local and national advice like Keeping Children Safe In Education, Teaching online safety in schools, Filtering and monitoring standards for schools and colleges and Cyber security standards for schools and colleges. The Online-Safety Policy and its implementation will be reviewed annually.

ACCESS TO THE INTERNET

Tonbridge School does all it can to monitor access to the internet via the School network. Access to the School internet has been designed expressly for the use of boys and includes filtering appropriate to the age of the boys. The School uses Smoothwall, a filtering system that blocks sites that fall into categories such as self-harm, substance abuse, pornography, racial hatred, extremism, and other sites of an illegal nature or containing material unsuitable for boys. No device, whether School owned or personal, can meaningfully access the internet through the School's system without going through the Smoothwall filtering system. Access to the internet for boys and staff is governed by the Acceptable Use of Computers (Boys) Policy and IT Acceptable Use (Staff) Policy which lay down the framework within which the School network can be accessed and clear guidelines about staff and boy behaviour in relation to the internet and the use of the School network. The security of the School information systems will be reviewed regularly, and virus protection is updated on a regular basis.

The following measures are in place to support filtering and monitoring:

- The Designated Safeguarding Lead (Mr C. J. C. Swainson) is responsible for filtering and monitoring at Tonbridge School;
- Under the overall oversight of the Governors' Pastoral Committee;
- The IT Operations Manager (Mr David Mills) is responsible for the operation of the filtering and Monitoring system, Smoothwall, and the production of the daily safeguarding monitoring report for the DSL;
- The DSL decides when there are safeguarding concerns which are recorded on CPOMS along with subsequent actions. These can be reviewed at any time.
- Where staff and boys feel that the blocking of a particular site is impeding teaching and learning a request can be made to ITD, who in consultation with the DSL where necessary, will decide if a particular site can be unblocked. This is recorded on the Helpdesk ticket system.
- The IT Operations Manager tests the system every half term, or when an additional risk has been identified, there has been a change in working practice or a new technology has been introduced;

The DSL and the IT Operations Manager will meet at least annually to review the systems or when an additional risk has been identified, there has been a change in working practice or a new technology has been introduced. The School accepts the fact many boys may have unlimited and unrestricted access to the internet via mobile phone networks and/or the use of a VPN and takes appropriate steps to minimise the risk this poses like restricting the use of mobile devices, as set out in the Mobile Phone Use Policy, checking for VPNs, and reminders to staff, as part of their safeguarding and online safety training, of the need for continuous vigilance.

The School will search a boy's device, or devices, wherever suspicion arises that boys may have brought harmful online content into School on a device or used Mobile Data download it, thereby bypassing the School's filtering and monitoring systems,

Housemasters ensure that boarders in the Novi, Second Year and Third Year do not have access to their devices overnight.

The School takes all reasonable steps to ensure that the copying and subsequent use of internet derived materials by staff and boys complies with copyright law, and boys will be taught to be critically aware of the materials they read. They will also be taught to acknowledge the source of information used. Boys and staff are granted access to the internet by agreeing to the terms of the Acceptable Use of Computers Policy. Any student or staff member who breaches these terms may have access to the internet withdrawn.

The School takes steps to reduce the risks associated with inappropriate online behaviour and material. The internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace. Emerging technologies will be examined for educational benefit with oversight from the Deputy Head Pastoral, the Director of Learning, the Director of IT & Digital and Academic Enrichment and Heads of Department. The School takes all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur in a School setting or on a School computer or device.

Any material that the School believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

E-MAIL

Boys and staff are inducted into the appropriate use of e-mail and there is clear guidance in the above policies about what is and is not acceptable in terms of e-mail communication. Any inappropriate email must be reported immediately to ITD and the Deputy Head Pastoral and, where appropriate, to the Housemaster.

SOCIAL NETWORKING SITES

The School will block access to most social networking sites during the following times:

Mon-Fri:	0830 – 1800 1900 – 2100, 2200 – 0600*
Saturday:	0830 – 1600, 2200 – 0600*
Sunday:	1900 – 2100, 2200 – 0600*

Boys are advised never to give out personal details of any kind which may identify them and / or their location. No information may be posted which identifies the School with unacceptable opinions or activities, or which would bring the School into disrepute. Members of staff are advised not to run social network spaces for boys' use on a personal basis and must not 'friend' any current boy from a personal account except when agreed on a School trip and where two members of staff are present on the group, one of which is the group administrator. Boys and staff are advised to always keep their profile private. Where social media is being used as an educational tool, Departments should establish official accounts and not use their personal profiles. Staff should refer to the guidance on social media and digital communication and liaise with the Head of Communications.

CYBER-BULLYING

The internet and social networking sites must not be used to intentionally or deliberately hurt, humiliate, slander or defame another person. Boys are made aware that actions in this regard undertaken outside of School may also contravene School policy and be subject to School sanction (in the first instance). The same sanctions will apply to incidents of cyber-bullying as would apply to any other form of bullying. This includes bullying via text message, via instant-messenger services, Apps and social network sites (such as Snapchat, Instagram, Facebook or Twitter), via email, and via images or videos posted on the internet or spread via mobile phone or via Apps. It can take the form of any type of bullying, i.e., technology can be used to bully for reasons of race, religion, sexuality, disability, etc.

MOBILE COMMUNICATIONS AND EMERGING TECHNOLOGIES

Boys and staff are made aware that the guidelines which apply to the use of the School network also apply to any portable communication device such as mobile phones, tablets or laptops brought onto the School site. Nothing which is inappropriate or potentially illegal should be downloaded or saved onto these devices and all should be aware of the possible criminality of transmitting such material.

INAPPROPRIATE OR PROHIBITED SEARCHES BY BOYS

Complaints of serious internet misuse are handled by the Housemaster or Deputy Head Pastoral. All incidents of serious internet misuse are recorded and passed on the Second Master or Headmaster. Sanctions may be applied to boys who breach the Acceptable Use of Computers (Boys) policy.

RESPONDING TO ONLINE INCIDENTS AND SAFEGUARDING CONCERNS

All members of the School community are reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the School community or which bring the School into disrepute. All members of the community are made aware of the range of online risks that are likely to be encountered including youth produced sexual imagery (sexting), online/cyber bullying, sexual harassment, access to harmful content etc. This is highlighted within staff induction and training, and educational approaches for boys.

The Designated Safeguarding Lead (DSL) must be informed of any online safety incidents involving safeguarding and child protection concerns, which will then be recorded in line with other safeguarding, welfare or pastoral issues. The DSL ensures that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Multi-Agency Partnership thresholds and procedures. The School informs parents/carers of any incidents or concerns as and when required.

Any complaint about staff misuse is referred to the Headmaster and allegations against a member of staff's online conduct may lead to disciplinary action, and may be discussed with the LADO (Local Authority Designated Officer) team in line with procedures set out in the Safeguarding Policy and Staff Code of Conduct. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will consult safeguarding partners and contact the Kent Police via 101, or 999 if there is immediate danger or risk of harm. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

Parents and boys will need to, and are expected to, work in partnership with the School to resolve any issues that arise.