ACCEPTABLE USE OF COMPUTERS (BOYS) POLICY

Any large computer network is a highly complex system requiring a considerable amount of maintenance. The points below are designed to ensure that the network is always available and working at the appropriate times. All users of the network (whether using School computers, personal laptops or any other device that can connect to the School network by whatever means) are expected to use their common sense, the more general School rules and the law of the land. This policy also applies to any access to the internet or the School network using 3G, 4G or 5G, wireless or any other technologies whilst at School or under School control.

This Policy should be read in conjunction with the policies listed below:

- Safeguarding Policy
- Online-Safety Policy
- Cyberbullying Policy
- Anti-Bullying Policy
- Behaviour Rewards and Sanctions Policy
- Emerging Technologies and Use of New Media Policy
- Confiscations Policy
- Privacy Notice for Boys
- Mobile Phone Use Policy
- Taking Storing and Using Images of Pupils
- Guidelines for use of Email

SYSTEM SECURITY

Boys are responsible for their individual account and must never allow anyone else to use it, even when they are present. Passwords should be of sufficient complexity and must never be divulged to another person. Anyone who is concerned that the security of their account may have been compromised in any way must talk to their Housemaster or contact ICT Services.

UNAUTHORISED ACTIVITIES

Boys should not attempt to go beyond their authorised access. This includes attempting to log in through another person's account, sending e-mails while masquerading as another person, or accessing another person's files in their directory. No-one must make deliberate attempts to disrupt the computer system or destroy data. Boys should also not attempt to deceive other external secure websites through the School network. Any deliberate attempt to 'hack' into the School's ICT infrastructure or to deliberately evade or circumvent the School's firewall, for example by the use of a Virtual Private Network (VPN), will result in disciplinary action that may include Temporary or Permanent Suspension from the School.

SOCIAL NETWORKING SITES

Boys must not post personal information to social networking sites such as YouTube and Facebook or using apps such as Whatsapp, Snapchat, Instagram, TikTok and Twitter if such information would allow others find out details of where a person lives. Such services, used sensibly, can provide genuine opportunities for keeping up with friends, but everyone must be aware that other users may not necessarily be who they say they are. No-one must use such services to impersonate others, to send inappropriate or offensive images, nor to participate in any form of "cyber-bullying". Nothing must be posted on such services which identifies the School with unacceptable opinions or activities, or which would bring the School into disrepute.

E-MAIL

Boys are referred to the 'Guidelines for the Use of Email', appended to this Policy.

No indecent, obscene, offensive, or threatening language can be used, nor should anyone engage in personal, prejudicial, or discriminatory attacks. At all times, privacy should be respected concerning any messages sent and no messages should be re-sent or forwarded to others without permission. School emails should be checked frequently and unwanted emails deleted. Boys must use their School email addresses when emailing members of staff.

INTERNET ACCESS

Use of the School network is carefully filtered and recorded for Safeguarding purposes. Computers at School or other devices which can link to the School network or the internet whilst at School (or whilst under School control) must not be used to access material that is profane or obscene, that advocates illegal acts, violence, or discrimination towards other people, or encourages radicalisation or extremism. If inappropriate information is mistakenly accessed, the Housemaster or another teacher should be informed immediately. This action will protect boys against the accusation that the material was intentionally accessed. Boys must not plagiarise works found on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were one's own. Copyright must be respected. The internet must not be used to download illegal software or, for example, pirated music, images or films. No software or programmes may be installed on any School computer without explicit permission from ICT services.

DEVICES

The rules that apply to School computers also apply to boys' own devices when brought to School. Boys should ensure that any unsuitable material (as defined in the previous paragraph) is deleted before bringing it to School. Boys must not be allowed access to each other's devices. Technologies such as 3G, 4G or 5G, and wireless should not be used to gain unfiltered web access, nor may boys employ VPNs to breach or circumvent the Firewall. If there is a suspicion that a boy has broken these rules, the Housemaster or System Administrator may remove the boy's device without warning, prior to an investigation taking place in conjunction with the Deputy Head Pastoral or Second Master; this investigation would include the School searching a boy's device, or devices wherever suspicion arises. This approach is designed to help the School manage the risks presented by boys accessing harmful online content

RESPECTING RESOURCE LIMITS

Large files should not be downloaded or saved unless absolutely necessary. Boys should refrain from excessive use of Social Media platforms to send video footage or images. This also applies to the streaming of films or television via the School network as these activities can restrict others' use of the network. Boys should respect the age classification of films they are watching and games they might play.

PRINTERS

Printers at School should only be used by boys for the production of educational material related to legitimate educational or co-curricular activities at Tonbridge School. Boys should consider the necessity of printing material in accordance with responsible environmental awareness.

PRIVACY

Boys should expect only limited privacy in the contents of their personal files on the School system or on their laptop if used to connect to the system. The Second Master, Deputy Head Pastoral, System Administrators, the Housemaster, and parents or guardians have the right at any time to require access to a boy's School directory or laptop. As a general rule, boys should not store anything which they would feel uncomfortable justifying in front of any member of staff or their parents.

SANCTIONS

When using the School's system, boys may think that it is easy to break the rules above without the risk of detection. However, whenever the network is used, an electronic trace is left that can subsequently be followed. Depending on the severity of the offence, one or more of the following sanctions may be applied if a boy is found to have broken any of the above rules:

- A formal warning
- Suspension of internet access
- Suspension of computer system account
- Device confiscation (phone, tablet, laptop, PC etc)
- Formal School sanctions
- Temporary or permanent suspension from the School