St. Nicholas School Canterbury

Kent County Council kent.gov.uk

Acceptable Wi-Fi Use Policy
(Online Safety Policy - Appendix D)

For staff, visitors and pupils granted access to the school Wi-Fi Network

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools boundaries and requirements when using the school WiFi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

The school provides WiFi for the school community and allows access for education use only.

Staff are normally allowed instant and permanent access to the Internet Access on school-owned devices. They may also apply to the SLT and/or ICT Systems Management team for permanent permission to join the WiFI network without a time limit on their personal device, providing they have signed this policy and have up-to-date anti-virus and anti-spyware software.

Visitors and pupils may, if appropriate, gain access to the school WiFi system on a personal device, providing they have up-to-date anti-virus and anti-spyware software. They will need to apply to the SLT and/or ICT Systems Management staff for temporary access to the school 'Guest' account. The time limit on this service, and the password they will be given, is 24 hours.

1. The use of ICT devices falls under the school's Acceptable Use, online safety, Safeguarding, Health & Safety and Behaviour policies and the Staff Code of Conduct which all students/staff/visitors and volunteers must agree to, and comply with (as appropriate).

2. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. School owned information systems, including WiFi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I will take all practical steps necessary to make sure that any equipment connected to the schools service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to,

any such instance of hacking or other unauthorized use or access into my computer or device.

6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.
8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
9. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.
10. My use of the school WiFi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
12. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Leads, the Online Safety Coordinators (Stephen King/David Jenner) and/or the designated lead for filtering (ICT Systems Management) as soon as possible.
13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online Safety Lead (Stephen King) or the Head Teacher.
14. I understand that my use of the schools internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the schools suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

As staff, students and visitors should not be using their personal mobile devices on school premises they should not be connecting to the internet via their own personal mobile broadband connections. As the above safeguards and agreements that are part of our school network security are not present when people are using 3, 4 or 5G providers nor are they possible to confirm/monitor mobile internet use during school activities is not allowed.

I have read and understood and agree to comply with the St Nicholas School WiFi Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name: