St. Nicholas School Canterbury

Acceptable Use of Technology Statement (including Internet, Digital Contact and ICT Equipment) for Staff, Parents, Visitors and Students

The computer systems - networks, VLE, Wifi internet service, email, ICT equipment - are owned & managed by the school. It is made available to students to further their education and for staff to enhance their professional activities including teaching, research, administration and management. Parents, partners and visitors may use school systems in order to enhance their communication with and experience of the school. The school's Internet Safety Policy has been drawn up to protect all parties – students, staff and the school.

Staff, students and visitors will act in a professional manner when using e-communications on or off-site, the school e-mail services/digital learning systems and in their social networking i.e. respecting sensitivities and confidentiality. The school email system should be used to contact colleagues, parents or other professionals – staff should not use their private or home email systems, in relation to school matters or their professional duties. NB: It will be considered a breach of confidentiality and (gross) misconduct for staff to discuss the events of the school, other staff and/or pupils in electronic communications including email or social networking – such breaches will be investigated and managed according to the school code of conduct. **It is not appropriate for staff to communicate with any pupil or family member via social networks or their personal mobile phones. It is strongly recommended that staff do not accept parents as *friends* via social networking systems or communicate with them by mobile phone (unless unavoidable e.g. due to emergency situations or residential visits). Video or photo sharing is prohibited.**

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff and students/parents requesting internet access should sign a copy of this Acceptable Internet Statement, when they first join the school, and return it to the ICT Manager for approval.

Staff may use of their own devices to support their work in school, but this must be in compliance with the Bring Your Own Device to Work policy guidelines (found within the Staff Code of Conduct Policy). Only laptops, tablets and/or USB drives owned by the school can be used within the school; these will be supplied to relevant staff and their use must be for professional and/or educational purposes only. It is the responsibility of staff to keep the anti-virus settings of their own/school-provided devices up-to-date and secure (via encryption, appropriately strong password, fingerprint technology) at all times. Staff are not allowed to install downloaded programs or personally owned software (.exe files) onto the school-owned laptop provided for them – unless given express permission by the Senior Leadership Team. Sensitive personal information or data files can only be saved to secure, encrypted cloud or mobile storage areas. Any abuses of the school ICT Network; email system, school owned laptop or other ICT equipment may result in temporary confiscation and loss of the item or misconduct/disciplinary procedures if appropriate. Where the abuse is illegal the incident will be reported to the police and/or any other relevant service.

Rules for use of the school internet and network systems:

- Access should only be made via the authorised account and (appropriately strong) password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden – any activity will be considered as gross misconduct.
- There is a zero tolerance of *cyberbullying* of any sort in or out of school; this will result in the loss of a school account and reporting to the senior school leader on duty, for action. This includes mobile phone use and social media. The posting of anonymous messages and/or forwarding of chain messages are forbidden. Any occurrence of *cyberbullying* or pupil misuse of the school network/internet systems will result in the loss of such privileges for a term and a parental interview with the Deputy Headteacher. All *cyberbullying* or *sexting* incidents must be reported
- Copyright materials must be respected and school-based information systems or hardware must not be used in the commissioning of any criminal offence – any computer misuse will be considered misconduct.
- Staff will maintain data protection at all times. Care must be taken with the use of USB pen drives, cameras and school laptops off-site. NB: All laptops and pen drives should be encrypted to maintain data security. Data protection violations will be considered gross misconduct.
- For safeguarding purposes, no mobile device - laptop, camera, USB drive etc. - will leave the school containing photographic or video images of the pupils. Any photographs of students taken (on cameras or mobile phones) will be transferred to the school system within 24hrs of the image being taken or on return to school, (if on a residential visit). No images of pupils or events during the school day/on school premises may be used on the personal social networking space of school staff or visitors. This will be considered gross misconduct and result in disciplinary procedures.
- The use of mobile technology to access the internet is prohibited within the school grounds (personal mobile phones, tablets, wearables – e.g. smart watches) as these internet devices and their usage cannot be monitored and, therefore, there *safety* cannot be assured. Pupils may only use phones to listen to music with specific permission (see mobile phone policy).
- All Internet activity should be appropriate to staff professional activities or the students education. Legitimate private interests may be followed where these cause no difficulties for other users and do not compromise school use. *Online shopping is not considered appropriate!*
- Use of the school internet system or equipment for personal financial gain, gambling, political purposes or advertising is forbidden. Information sharing (e.g. regarding services for parents) is permissible.
- The same professional levels of language should be applied when using email, particularly as they are often forwarded or may be sent inadvertently to the wrong person. Inappropriate use of the email system or inappropriate language within messages will be considered as misconduct and a disciplinary issue. School events or images included pupils must not be shared via social networks.
- Users must only access those sites and materials relevant to their work in school.

- The ICT Department and Systems Managers will periodically monitor the use of the school network, internet, ICT Equipment (inc. USB Drives, Cameras and USB Drives) and email systems. They reserve the right to monitor the user accounts of staff, visitors and students to maintain the integrity of the system. Users will be aware when they are accessing inappropriate material and should expect to have their permission to use the system removed for a temporary or permanent period. It will be considered gross misconduct for staff to use school equipment for the access, production or storage of sexually inappropriate material, illegally-shared music or video files. Where misconduct is suspected, the equipment will be investigated and, if inappropriate usage is found, the situation will be dealt with by formal disciplinary measures.
- All users accept that the content of their internet or school email use is subject to filtering and subsequent inspection should abuse or misuse be found.
- Staff accept that all school-owned equipment – laptops, mobile devices and USB storage are to be serviced and monitored for appropriate use 3 times per year. Any abuse or misuse will be considered misconduct.
- Staff, students and visitors will only be allowed access to the school computer systems once they have agreed, in writing, to adhere to this policy statement, by signing the form below.
- We operate a *screen lock* policy (when away from desk), to avoid any accidental data breach/confidentiality violation.

Full Name: ----------

Signature: ----------

Role (staff/student/visitor): ---------- Date ----------

Parents signature (if approp.) ---------- Date ----------

Access granted by: ---------- Date ----------

This policy statement is part of the school Internet Safety Policy. It complies with the Kent e-Safety policy and is to be made available to all who have access to school computers or have use of the school network and/or internet systems.