Acceptable Use Policy

This policy will be reviewed annually
Policy reviewed: August 2018 by SMT
Next review: August 2019 by SMT

Computing at WCPS

This policy reflects and complements the principles and practice outlined in the Behaviour policy, the Anti-bullying policy, the Safeguarding policy and the Data Protection policy. WCPS pupils are required to accept these rules as a condition of logging on to school facilities. They apply to all uses of fixed and mobile technologies, whether on or off-site; networked or standalone; school or personal devices; tablets or smart phones.
All our pupils should act with consideration, common sense and good manners at all times. Any violation of this policy should be reported to a teacher immediately.

User accounts
Pupils must never use a computer whilst logged on as another person

Classroom computers
Unsupervised pupils may not use computers in classrooms without permission.

E-mail

- Pupils must not use internet-based e-mail services (such as Hotmail)
- Pupils may not send e-mails which appear to be either anonymous or from another person
- Pupils may not send bulk e-mails (i.e. e-mails to more than five recipients) unless a teacher gives prior consent.

Internet

Network internet access is appropriately filtered. The school is mindful that this should not lead to unnecessary restrictions on learning, and any pupil who wishes to block/unblock specific sites should talk to their teacher. The internet may only be used for research related to academic subjects and individual study i.e. for educationally beneficial tasks rather than recreational use such as games. Pupils may not use ‘chat’ services.

Monitoring

Pupils should be aware that any use of the school network may be monitored to ensure appropriate usage. This includes the remote scanning of computer monitors, the checking of files and e-mails, and the analysis of internet sites visited. The school has a robust system (Smoothwall) for monitoring Internet searches and blocking websites and links which are inappropriate for pupils and staff to use while on school site. The system is managed by the ICT department and monitored by the senior management team. To ensure that flaws and gaps in the system do not arise, the firewall is challenged on a regular basis.

Online safety

Pupils are taught through PSHE to manage their digital footprints, respect their own privacy and that of others, and ‘think before they post.’ They are aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ guardian, teacher/ trusted staff member.

WCPS is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all pupils fulfil their potential.

Cyber bullying

Mobile devices and computers are a source of education, communication and entertainment. However, we know that some adults and young people may use these technologies to harm children. The harm might range from sending hurtful or abusive texts, messages and emails, to enticing children to engage in sexually harmful conversations online, webcam filming, photography, sexting or face-to-face meetings. These technologies may also be used by those who wish to radicalise vulnerable children for their violent purposes.

Pupils receive guidance on cyber safety and bullying through our PSHE programme. Pupil use of social networking sites, texts and e-mails should not be hurtful to pupils or staff, here or elsewhere, neither should it bring the School's name into disrepute. Cyber-bullying - that is, using the internet, mobile 'phones, social networking sites to deliberately upset someone else - is treated as seriously as any other type of bullying and is managed through our anti-bullying procedures. Pupil resilience is encouraged so that they can protect themselves and their peers. If you feel you or another pupil have been teased, bullied or threatened, it's never too late to tell a teacher or parent.

Offensive material

Pupils must not use ICT to view, send or store offensive material, including extremist websites which could incite hatred or violence. If such material is seen or discovered, or viewed by a friend, it should be reported immediately to a teacher.

Hacking

Hacking is illegal and is forbidden. This includes attempting to gain access to any file, function or network area which a pupil does not have permission to view or use. Pupils must not attempt to bypass monitoring software.

Mobile devices

Pupils are not allowed to use mobile devices anywhere in the school or to bring mobile devices in to school.

Printing

- Pupils must take care not to print excessive amounts, nor to waste paper
- Pupils must obtain a teacher's permission before printing a poster, or a file on a colour printer
- If a file does not print, pupils should check that there is paper loaded in the printer. If it still does not print, they should cancel the print job from the queue and report the problem to a teacher.