ALLESTREE
WOODLANDS
SCHOOL

ACCEPTABLE USE POLICY

DATE OF POLICY ADOPTION BY GOVERNORS:	February 2020
AUTHOR/S OF POLICY:	Greg Duffy
DATE OF LAST REVIEW:	February 2020
DATE OF NEXT REVIEW:	January 2021

Acceptable Use of IT at Allestree Woodlands School:

This IT Acceptable Use Policy helps protect students, staff and the school by clearly stating what is acceptable and what is not. These statements refer both to computer equipment based in school and to school laptops assigned for use both at school and at home. For personal computing equipment (including smartphones, tablets and laptops) please see the Mobile Phone Policy.

- School computer and Internet use must be appropriate to the student's education or staff professional development.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made.
- E-mail should be written carefully and politely. As messages may be forwarded, e-mail is to be regarded as school and therefore public property.
- Users should not use IT systems or devices to cause harm, humiliation or injury to others; this includes the taking of and/or distribution of pictures under a person's clothing i.e. upskirting.
- Do not send, attempt to access, save or display offensive messages or pictures. If any such material accidentally appears inform a member of staff immediately.
- The use of public chat rooms is not allowed.
- Use of the ICT facilities for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, do not attempt to access areas that you are not allowed to, this is hacking.
- Irresponsible use of the ICT facilities may result in disciplinary action being taken.
- Treat the equipment with respect. Always inform a member of the ICT technical team if there is something wrong. Never attempt to fix a problem yourself.
- Please be very aware that the school will exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of staff laptops, web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.
- Online information will be filtered to prevent access to inappropriate, offensive or illegal content; including extremist content. The school will sanction appropriately the creation of or attempt to access unauthorised, unlawful or offensive materials; liaising with external agencies, including the Police, CEOP, Prevent etc., as appropriate and in-line with the safeguarding policy.
- Staff should not use personal email or other personal communication or social networking systems to communicate with students. Staff should only use staff school email or other school approved systems for communication with students. Other online educational systems may be used (e.g. BrainRush or Khan Academy) but staff should register their accounts with ITServiceDesk. These systems will fall under the same monitoring and access arrangements as described above.

In line with our responsibilities under the General Data Protection Regulation (GDPR)

- Staff must use strong passwords and keep them secret. If a password becomes known to students you should change it immediately. Please contact ITServiceDesk for assistance
- Students must not be allowed to use staff password or access to school systems e.g. printing, SIMS etc.
- School devices and accounts should not be left open or logged-in while unattended. Lock devices when they are unattended e.g. using the Ctrl+Alt+Del functions on a school desktop or laptop.
- Staff should not take any un-encrypted electronic pupil data off-site. This includes data stored on laptops, or portable storage devices like external hard-drives. It is possible for these portable devices to be encrypted; please contact ITServiceDesk for details.
- Cloud storage systems that use storage in the USA e.g. Drop Box must not be used for storing pupil data. This is because the US Patriot Act conflicts with the UK Data Protection Act. Staff may use US Cloud storage systems for non-pupils level data e.g. worksheets and learning resources.
- When staff make use of systems that allow online/wireless access to student data on portable devices they must use a password lock to secure their device when unattended and should enable additional security applications such as “Find iPad/iPhone” where available. Such applications should not be accessed via unsecured or public wireless access systems. Home wireless systems should be password protected and additional available security settings enabled.

Bringing Personal IT devices into school

Allestree Woodlands School ITServiceDesk staff will not service, repair, or maintain any personal devices. Allestree Woodlands School will not be held liable for personal content stored on the personal devices. Any software residing on personal devices must not interfere with the normal operation of school owned resources and must be properly licensed. Allestree Woodlands School is not responsible for any physical damage, loss, or theft of personal devices. Personal internet usage or texting charges are the responsibility of the student. Students are responsible for taking their personal devices home each day and returning the next day with a full charge. Allestree Woodlands School will not offer charging facilities for personal devices. Students are responsible for keeping personal devices in a secure location when not in use. Student use of personal devices must support the learning activities in lessons and must be turned off and put away without question when requested by a teacher. Students may use personal devices out of lesson time but should be aware that:

- Personal and school devices must be used in-line with the Mobile Phone policy.
- While a personal device is connected to the Allestree Woodlands School wireless school filtering will be applied and violations will be traceable to that student.

- If students access the internet using their own 3G and 4G data at school then they must follow the same rules that apply for accessing the internet using the school's Wi-Fi. When accessing the internet in lessons using their own devices students must use the school wi-fi and not their own data.

- In line with the Keeping Children Safe in Education 2019 students must also not access inappropriate, offensive or illegal content on the internet; including extremist content using their own 3G or 4G data. Parents and carers will be informed that it their responsibility to set appropriate 'Parental Controls' on their children's mobile devices before they bring them into school. The school will sanction appropriately the creation of or attempt to access unauthorised, unlawful or offensive material and liaise with external agencies, including the Police, CEOP, Prevent etc., as appropriate and in-line with the safeguarding policy.

- Failure to comply with the BYOD policy will result in fixed-term removal of access to school wireless in addition to other appropriate sanctions e.g. confiscation of the mobile device and contact with home including details of any inappropriate activity.

- Persistent failure to comply with the BYOD policy will result in the confiscation of the mobile device and permanent removal of access to school wireless in addition to other appropriate sanctions.

- Students must keep their username and password secret. Student's school username and password will allow access to the school wireless network.

- Students are not permitted to use the username and password of another student or staff member

- Allestree Woodlands School reserves the right to ban students from using their mobile devices in school and limit or remove student access to school wireless without prior notice as necessary to facilitate the efficient running of the school network.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child Protection Policy
- Online Safety Policy
- Code of conduct for staff and volunteers
- Anti-bullying policy
- Photography and image sharing guidance

Contact details

Online safety co-ordinator
Name: Greg Duffy
Email: g.duffy@woodlands.derby.sch.uk
Senior lead for safeguarding and child protection

Name: Rachel Brailsford
Email: r.brailsford@woodlands.derby.sch.uk

We are committed to reviewing our policy and good practice annually. As part of this review students are consulted through focus groups to determine that e-safety content is appropriate to their context and needs and delivered at the most effective point in their school journey.