THE KING'S SCHOOL
CHESTER

Pupil ICT Acceptable Use Policy

Policy owner	Pastoral Deputy Head
Last reviewed by **Date**	Pastoral Deputy Head September 2021
Last approved by **Date**	Full Board Annual Safeguarding Review September 2021
Next policy review by owner *(annual)*	September 2022
Next policy approval by governors	Safeguarding group September 2022 *Followed by:* Full Board Annual Safeguarding Review September 2022
Circulation	All staff and governors, school website, Firefly
Linked policies	Behaviour Policy Child Protection and Safeguarding Policy Online Safety Policy
ISI regulatory requirements	**Part 2** Paragraph 5(b)

Contents

Appendices

1. Introduction

The King's School is committed to the effective and safe use of ICT (Information and Communications Technology). Pupils have access to the school's ICT services and this brings with it the responsibilities as outlined below.

This policy applies to the use by pupils of devices and services provided by the school and to pupils who connect their own devices to the school network. The use of mobile phones (cellular 3G, 4G and 5G etc devices) is covered in Appendix 1.

This policy is shared with pupils during their induction and they are required to acknowledge their agreed compliance with the service agreement each time they log onto the network (see Appendix 2).

Any person who is aware of a breach of this policy should report their concerns to a member of staff, or if a safeguarding concern, they should report this directly to the Designated Safeguarding Lead (DSL) in line with the school's safeguarding procedures.

A summary of this policy and guidance is included in the Student Handbook.

2. Purpose of policy

The purpose of this policy is to:

- Outline the acceptable and unacceptable use of ICT equipment and services in the school
- Safeguard and promote the welfare of pupils, in particular anticipating and preventing the risks arising from;
    - Exposure to harmful or inappropriate online content
    - Sharing of personal data and images
    - Inappropriate online contact
    - Cyberbullying and other forms of peer-on-peer abuse.
- Help pupils take responsibility for their own safe use of ICT
- Ensure that pupils use ICT safely and securely
- Educate and encourage pupils to make effective use of the educational opportunities presented by access to technology

3. Scope of policy

This policy applies to all pupils of The King's School.

The policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:

- The internet
- Email
- Learning platforms, including Firefly and Office 365 (Microsoft Teams, OneNote etc)
- Mobile phones including smartphones
- Tablets, laptops and desktops
- Interactive boards and screens
- Devices capable of recording and/or storing images
- Wearable technology

This policy applies to the use of this technology on the School premises and it also applies to the use of technology off the school premises where the use involves harm to pupils or any member of the school community or where the reputation of the school or member of staff is brought into disrepute.

4. Safe use of technology

Pupils should be able to enjoy using ICT and become skilled users of online resources and media.
The school will support pupils to develop their skills and provide internet access whilst balancing the safety and welfare of pupils and the security of our systems.

Pupils are educated about the importance of safe and responsible use of ICT to help them to protect themselves and others online. Pupils may find the following resources helpful in keeping themselves safe online: www.thinkuknow.co.uk, www.childnet.com. Further links and resources are provided on Firefly.

Pupils are responsible for their actions, conduct and behaviour when using ICT at all times. If a pupil is aware of misuse by other pupils, they should report this to a member of staff as soon as possible. Any misuse of ICT by pupils will be dealt with under the school's behaviour policy. Pupils must not use their own, or the school's ICT to bully others. Such behaviour will be dealt with under the school's Anti-Bullying Policy.

If any case gives rise to Safeguarding concerns, the matter will be dealt with under the school's Child Protection and Safeguarding Policy. In a case where the pupil is considered to be vulnerable to radicalisation, this will be dealt with under the Prevent Programme.

5. Unacceptable Use

The school provides internet access, learning platforms and an email system to pupils to support their learning and development.

Unacceptable use of ICT may be summarised as, but not restricted to:

- Action/s which causes physical damage to any ICT hardware including associated equipment.
- Action/s which cause damage, loss, or theft of devices through negligent, irresponsible or careless behaviour
- Attempting to break into or damaging computer systems or data held, including attempts to access systems or data for which the individual is not authorised
- Creating, displaying or transmitting material that is fraudulent, or otherwise unlawful, likely to cause offence, or inappropriate
- Viewing, retrieving, downloading or sharing any offensive material which may include content that is abusive, racist, considered to be of an extreme or terrorist nature, sexist, homophobic, pornographic, defamatory, or criminal activity
- Using ICT for purposes of gambling
- Using ICT to threaten, intimidate, bully or harass staff, pupils or others, including prejudice-based or discriminatory communications
- Intellectual property right infringement, including copyright, trademark, patent, design and moral rights
- Sending messages or emails that purport to come from an individual other than the person sending the message
- Action/s or inaction/s which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, including the use of equipment which is inadequately protected against viruses or spyware.

6. Photographs and images, including Youth Produced Sexual Imagery

The following applies more specifically to the production, use and distribution of photographs and images (which includes video clips):

- Pupils may only use cameras or mobile electronic devices to take images in school and/or during school activities with the express permission of a member of staff and with the permission of those appearing in the image
- Pupils must allow staff access to images stored on mobile devices and must delete images if requested to do so. This does NOT apply to nude and semi-nude images which must neither be viewed nor deleted.
- Any pupil who receives an inappropriate or unauthorised image should immediately speak to a member of staff
- The posting of images which are considered by the school to be offensive or brings the school into disrepute is a serious breach of discipline and will be subject to sanction whether the image was posted using school or personal devices
- The use of images of any kind to bully, harass or intimidate others will not be tolerated and constitutes a serious beach of the Anti-Bullying Policy.

It is important to remember that once a photo or message is sent, the sender has no control regarding its subsequent distribution. Even if the image is deleted, it could have been saved, copied or shared by others. Images shared online become public and may never be completely removed.

The consensual and non-consensual sharing of nude and semi-nude imagery is a serious issue whether or not the pupil is in the care of the school at the time the image is recorded and/or shared. Such actions may also constitute a criminal offence even if the image is taken or shared with permission of the person in the image.

It is strictly a safeguarding matter and must be reported to the DSL. Full guidance is provided in the Child Protection and Safeguarding Policy.

7. Sanctions

Where a pupil breaks any of the rules, practices, or procedures set out in this policy, the school may apply sanctions which are appropriate and proportionate in accordance with the school's Behaviour Policy and Online Safety Policy including, in the most serious cases, permanent exclusion.

Unacceptable use of electronic devices or the discovery of inappropriate data or files could also lead to the confiscation of the device or deletion of the material.

8. Access and security

Pupils must not use or attempt to use ICT resources or materials stored on ICT systems belonging to others except when explicitly authorised. Any attempt to access any user account or email address for which the pupil is not authorised is prohibited.

The school has a filtering system in place to block access to unsuitable material to protect the welfare and safety of pupils. Pupils must not try to bypass this filter by using VPNs or other technologies. The school also uses monitoring software to automatically identify when keywords, phrases, abbreviations or acronyms are typed anywhere on student accessible computers on the school network.

Viruses can cause serious harm to the school's network and are often spread through internet downloads or circulated as attachments to emails. If a pupil thinks that an attachment or other downloadable material

might contain a virus they must speak to a member of IT support before opening the attachment or downloading the material. Pupils must not attempt to disable or uninstall antivirus protection on the school's computers.

The allocated username and email address are for the exclusive use of the individual for whom they are allocated. Pupils should have a PIN or passcode on their devices to protect their information if the device is lost, stolen or accessed by others. Passwords connected to a particular username must not be divulged to others. If it is suspected that they have become known to others they should be changed immediately.

For the protection of all pupils, their use of email and the internet when accessed via the school network will be monitored by the school. Pupils should remember that even when an email or downloaded information has been deleted it can still be traced on the system. Pupils should not assume that any files stored are private to the individual. Pupils should lock or logoff from school computers when they have finished using them to ensure others cannot access their accounts.

9. Use of the internet, email and Teams messaging

It should be noted that use of the internet and emails are monitored by the school to ensure the safety of pupils and staff and adherence with this policy.

The following applies more specifically to the use of the internet, email and Teams messaging:

- Pupils must take care to protect personal and confidential information about themselves and others when using the internet
- Pupils must not view, download, or share any offensive material. Using ICT in this way is a serious breach of discipline and may constitute a criminal offence. Pupils must inform a member of staff immediately if they have accidentally downloaded or have been sent any offensive material
- Pupils must always use their school email accounts for any email communication with staff. Use of personal email accounts for this purpose is not permitted
- Pupils must not read anyone else's emails without their consent.
- Pupils must not communicate with staff using social networking sites or other web-based communication channels unless this is expressly permitted by the staff member
- Email should be treated in the same way as any other form of written communication. It should be remembered that emails can be forwarded to or seen by others to whom they were not originally sent.
- All pupils must abide by laws relating to the use and protection of copyright.
- Teams messages should be treated in the same way as any other form of written communication.
- Teams messages cannot be deleted once sent for audit purposes and should be used for school related queries and discussion only.
- Messages within teams should not be used as a personal social media platform for communication between pupils.

10. Mobile electronic devices

All pupils are permitted to connect their devices to the school's wireless 'guest' network which plays an integral part of their access to learning and teaching.

Any mobile device, including wearable technology, may be confiscated in appropriate circumstances.

The school does not accept any responsibility for the theft, loss or damage to mobile electronic devices brought into school including devices which have been confiscated or handed into staff.

Appendix 1: Mobile phone and wearable technology policy

Mobile phones

It is accepted that mobile phones have become a part of everyday life and it is also recognised that associated (and/or standalone Cellular enabled) wearable devices are also becoming common place.

Children in Willow Lodge, including EYFS, are not allowed to bring mobile phones into school.

Pupils in The Junior School may only bring mobile phones into school by prior arrangement with the Head of The Junior School. This would normally only be permitted for a valid and specific reason involving their travel to and from school and their mobile phones will be locked away during the school day.

All Senior School pupils are permitted to bring a mobile phone in to school. For Removes to Fifth Year, these devices should be turned off during the school day and kept in lockers. Sixth Form students may use their mobile phones in the Sixth Form Centre during the school day and to support learning in lessons with the permission of their teachers.

Junior school pupils are not allowed to take mobile phones on trips or visits. For Senior School pupils, permission for use of phones and wearables on trips and visits will be communicated on a per trip basis.

Pupils must not communicate with a member of staff's personal mobile phone.

Wearable technology (including 'smart watches')

Our strong advice is that pupils should not bring any wearable technology into school, given they may cause unnecessary distractions to pupils and staff, especially within lessons. If wearable technology does cause any such distraction it is liable to confiscation by staff until the end of the school day. Sanctions for the misuse of wearable technology are consistent with those for the misuse of mobile phones.

If they are brought into school, wearable technology devices must be set to 'do not disturb/flight mode' throughout the working day.

Wearable technology must not be worn in examinations as exam regulations do not permit any device capable of mobile communication or data storage. Anyone found with any wearable technology device in an exam is likely to be disqualified from that exam.

Appendix 2: ICT services agreement - pupils

Each time you log in to the school network either on a school device or on your own device, you agree to the following rules:

- *I understand that school ICT equipment must be used responsibly, and I understand that the school may monitor the way I use the equipment and school network to make sure I follow these rules.*
- *I understand that the school will provide filters to block certain content that is unsuitable, and I will not use VPNs or other software to bypass these filters.*
- *I will respect copyright and intellectual property rights and will not store or share illegally downloaded materials*
- *I will not try to install any software or hardware.*
- *I will not connect any equipment to the school's wired network without permission.*
- *I will respect the security of the school network and I will not disclose any password or security information to anyone.*
- *I will ensure that all personal data is kept secure and is used appropriately.*
- *I will report any worries or concerns regarding the online safety of myself or others to a member of staff.*
- *I will ensure that any electronic communications with staff are appropriate and occur via an authorised school email address or via the schools learning platforms.*
- *I will not use the school equipment or network to communicate with other students unless it is for an educational purpose.*
- *I will not invite members of staff to be a contact or attempt to follow them on any personal social networking sites*
- *I will not publish information publicly if it compromises the position of the school.*
- *I will follow online safety advice and develop a responsible attitude to system use and to the content I access or create.*

The school may exercise its right to monitor the use of the school's technology, including data stored on the school network, internet access and email.

The school will take the necessary action where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.