KING EDWARD VI
HIGH SCHOOL FOR GIRLS

Pupils' Acceptable Use of ICT including Mobile Phones, Smart Technologies and Electronic Devices

Committee	**N/A**
Policy Type	**School**
Policy Owner	**Senior Deputy Head (Pastoral)**
Statutory	**No**
Published on website	**Yes**
Last review date	**07/2025**
Next review date	**07/2026**
Review Cycle	**Annual**
Expiry date	**N/A**
Version	**1.0**

September 2025

Contents

1. Introduction

This policy relates to all pupils at KEHS and should be read in conjunction with the school's Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy.

2. Aim and scope of this policy

The aim of this policy is to ensure that:

- pupils will be responsible users and stay safe while using the internet and other digital/ smart technologies for educational, personal and recreational use
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

The school provides its pupils with access to the school network and internet to enhance pupils' education and learning. The school network, internet and smart technologies can offer great opportunities for learning, but also, of course, opportunities for inappropriate behaviour and access to material that may be harmful or offensive or unsuitable for other reasons. Whilst we operate a school filtering and active monitoring system, it is essential that pupils behave responsibly when using computer equipment, smart technologies or accessing the internet.

3. Promoting safe use of technology: the role of staff and pupils

Online safety training for staff is provided as part of our overarching approach to safeguarding children and staff reinforce online safety messages in all aspects of school life. We aim to build resilience in our pupils to enable them to protect themselves through education and information.

Digital learning is a component of every academic subject and many co-curricular areas; it is also taught as a subject in its own right. When available, pupils may use the machines in the Computer Room and in the Library for private study. Sixth Form students may also use the computers in the Sixth Form Common Room.

All pupils are taught how to research on the internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different sites and understand that some apparently authoritative sites need to be treated with caution.

Pupils in Year 7 complete a unit of work on Internet Safety, focusing on how to behave responsibly online, staying safe online, managing passwords and cyberbullying. These topics are revisited regularly as pupils progress through the school and new ones, such as the risks and consequences of sharing nudes and semi-nudes, are introduced through the PSHE programme, tutor time and assemblies. Topics are always covered to a level appropriate to the age and stage of the pupils. Pupils are taught about the risks of being radicalised online, particularly through their use of social media, in keeping with the Prevent Duty.

We know that pupils will, in general, always behave responsibly, courteously and with due regard to the law. Nevertheless, it is helpful to lay out clearly some things which are unacceptable. At the start of each academic year pupils sign to show their acceptance of the agreement contained in Section 6 of this policy; a signed copy of the agreement is kept by the DSL for future reference. Pupils are

frequently reminded of the commitment they have made to uphold high standards of behaviour and responsibility in their use of technology.

Our Designated Safeguarding Lead is aware of the safety issues involved with the misuse of the internet and smart technologies. The DSL works closely with Birmingham Safeguarding Children's Partnership (BSCP) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of KEHS. The DSL line manages the Head of PSHE, who ensures that all pupils in the school are educated in the risks and the reasons why they need to behave responsibly online. She liaises regularly with the Head of Computer Science to ensure online safety education is mapped across the curriculum.

The DSL monitors pupil use of the internet in School. It is the DSL's responsibility to handle allegations of misuse. The school network uses Smoothwall systems for filtering and active monitoring. Any required action following a pupil's inappropriate use of the network is recorded in CPOMS along with any interventions required to protect the pupil from harm and the support and guidance offered to the pupil to encourage safer and more responsible use in the future.

Our mobile phone rules are designed to ensure that pupils in Years 7 to 11 do not use their phones during the school day; we are aware that some parents have given their children access to the internet via mobile phone networks (i.e. 4G and 5G) and therefore we have carefully considered how this is managed on school premises in our approach. Pupils in the Sixth Form are given greater freedoms, to help prepare them for the world of work and university, but are strongly encouraged to use the school wifi on any smart device they bring in, to ensure adequate filtering is in place.

Our technical staff are responsible for maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware, software and our data and for training our teaching and administrative staff in the use of ICT. They regularly liaise with the DSL to strength test the filtering and active monitoring systems KEHS employs.

4. Searching electronic devices

If a member of staff has good reason to believe that an electronic device has been, or could be, used to cause harm, disrupt teaching or break school rules (not involving youth produced sexual imagery), they will refer the matter immediately to the Head of Year; they may also first confiscate the device. If the Head of Year feels that the device needs to be searched, they will refer the matter to the Senior Deputy Head or Assistant Head (Pastoral) who will follow the DfE guidance: Searching, Screening and Confiscation: advice for schools.

If a member of staff has good reason to believe that a personal device has been used for sending nudes or semi-nudes, they will refer the matter immediately to the DSL without confiscating or searching the device. The DSL will then follow the guidance published by the UK Council for Child Internet Safety: Sharing nudes and semi-nudes: advice for education settings working with children and young people.

5. Working with parents and carers

We seek to work closely with parents and carers in promoting a culture of online safety; we recognise that they play a crucial role in ensuring that their child understands the need to use the internet/ smart technologies in an appropriate way. We will always contact parents if we have any worries about a pupil's behaviour in this area, and we encourage parents to share any worries they

have with us. We are supportive of those parents/ families who make the decision not to give their child access to/ ownership of a smart phone.

We recognise that not all parents and carers may feel equipped to protect their children when they use the internet and smart technologies at home. The school takes every opportunity to help parents understand these issues through parent information evenings, newsletters, leaflets, emails and the school website. The school website hosts links to high quality information for parents about their children's wellbeing and resilience, much of which covers internet safety. The aim is to help parents ensure their children are discriminating consumers of online content, digitally literate, responsible and resilient.

Parents are encouraged to support the school in promoting good online safety practice and are asked to read this policy with which all pupils must comply.

6. Acceptable Use Policy Agreement

I understand that school computers, and internet access, have been provided to help me with my education and learning. I understand that I must use the school ICT systems, and personal devices, in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

6.1 For my own personal safety and that of others:

- I recognise that the school will actively monitor my use of school equipment and the school network. This includes tracking and recording sites visited, searches made, and emails sent and received by individual users.
- In school, I will only use social media sites for educational purposes; if this is during lesson time, then it must be with permission from a teacher.
- I will not post personally identifiable information about myself or other people anywhere visible to the public. This includes passwords, emails, names, home and school address, together with telephone numbers, age, sex, educational details, financial details etc.
- I will not take or distribute images of anyone without their permission.
- I will not post information about other people anywhere without their permission.
- I will not agree to meet with someone I have 'met' online without my parents' full knowledge and approval.
- I will not post, use or produce images which are obscene, vulgar, inflammatory, threatening, nor will I post or use language that is disrespectful of or harmful to others.
- I will not send offensive or harmful material to other users.
- I will not publish anything that I know to be either false or harmful about the school, its staff, my fellow pupils or their parents.
- I will not participate in acts of cyberbullying. If I see or hear of any evidence of cyberbullying, I will report it immediately to a member of staff.
- I will not use the school's name, initials or branding to label or promote campaigns, initiatives or events on social media sites or other places (for example, in an Instagram account name), without permission from the Senior Deputy Head.
- I understand that everything I do online creates a 'digital tattoo'. Just like a real tattoo, a digital tattoo is easy to create but extremely difficult to remove.

6.2 Use of internet, the school network and digital equipment – for the protection of pupils, others and the school:

- I will write emails and online messages carefully and politely.
- I will look out for suspicious emails which seem to come from someone I know but may actually come from a computer hacker.
- I will avoid clicking on links or attachments unless I am sure the message/ content is genuine.
- I will not use any programmes or software that might allow me to bypass the filtering/ monitoring/ security systems in place.
- I will not engage in acts of plagiarism (i.e. claim the work of another as my own; see further information on AI generated content in the AI Policy).
- I will respect the law of copyright both in respect to printing of copyrighted documents, images, visual material, use of music or video files and use of software that belongs to other people in ways which are forbidden by law.
- I will not tamper with school digital equipment in any way.
- I will not use someone else's username or password to gain access to the school network, nor allow someone else to use mine.
- I will not leave a machine logged on and unattended.
- I will not search for security problems, whether real or imagined.
- I will not try to hack into unauthorised areas and I will not try and access parts of the system to which I do not have access.
- I will not carry out any act that might disrupt or harm the operation of digital equipment or the school network. I will not install or run any unauthorised form of software on the school network, try to alter computer settings, nor will I introduce viruses.
- I understand that the use of USB devices is not permitted.
- I will not access, copy, remove or otherwise alter the file space of another user or change the desktop settings without the owner's knowledge and permission.
- I will not send emails to staff via private (i.e. non-KEHS) email accounts.
- I will not send friend requests to staff on social networking sites.

6.3 Use of Personal Mobile Devices and Smart Technologies

The KEHS community believes it is important for pupils to spend time interacting with one another, relaxing, or participating in co-curricular activities at recess and lunch time. Whilst mobile phones and smart technologies are hugely beneficial in many respects, we do not consider their use during the school day to be necessary. Pupils are not permitted to wear smart technologies such as smart watches or rings, capable of sending and receiving messages or accessing the internet, to school.

Thirds to Upper Fifth

Mobile phones must remain switched off and out of sight from 08.30 until the end of the school day. If there is an urgent need to contact a parent during these hours, pupils must seek permission from any member of staff; if permitted, the use will be supervised. Pupils are able to use school landlines in an emergency. Where pupils do bring a personal mobile device to school, their use is subject to the following rules:

- Before 08.30 mobile phones may be used in the form room, or outside the buildings. No member of the school community should be disturbed by their use. After school mobile phones may be used except in corridors.
- Headphones must not be worn on the school site at any time, unless a teacher has given permission for this.

- Kindles and e-readers may be used before school, at recess, at lunch time and after school. They may only be used in tutor time and lessons with the permission of a teacher. Backlit devices such as a mobile phone may not be used as an e-reader.
- Mobile phones and other electronic devices may not be used on school trips without permission from a member of staff. Trip leaders will make expectations clear in advance of the trip.
- Use of electronic devices/ smart technologies of any kind, to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline, whether or not the pupil is in the care of the school at the time of such use.
- Mobile phones may not be used whilst at school or on a school trip to make direct contact with parents about an accident, illness or any other matter affecting a pupil's welfare; in this situation, pupils must report to the School Nurse (or other member of staff) who will decide upon the best course of action.
- Pupils may never use a personal mobile device on site to take photographs or make videos.
- Staff may confiscate mobile phones, where use has contravened the rules, until the end of that school day. It is the student's responsibility to collect a confiscated device from Reception promptly at the end of the day.
- Repeated breach of the rules will incur greater sanctions. A parent may be asked to collect the confiscated device for example, or a pupil may be required to hand their device in to Reception upon arrival each day.
- The school does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices/ smart technologies brought onto school premises.
- In an emergency, common sense should prevail.

Sixth Form

- Mobile phones may be used during study periods, recess and lunch time in the Sixth Form Common Room or outside the buildings (away from car parks). Only silent use is permitted in the KEHS Library (use is not permitted in the KES Library), which means that calls cannot be made or taken there. Sixth Form pupils may make safe and considerate use of social media sites. No member of the school community should be disturbed by the use of personal devices.
- Sixth Form students may be permitted to use their mobile phones in lessons if given the express permission of a teacher.

6.4 Reporting incidents of misuse

- If I receive any material which I think is inappropriate or which makes me uncomfortable, I will immediately inform a member of staff.
- If I gain access to, or have knowledge of others being able to access, a site which I think is inappropriate or which makes me uncomfortable, I will immediately inform a member of staff.
- If I have knowledge of any misuse of the school ICT systems by any user, I will immediately inform a member of staff.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to a member of staff.

6.5 Sanctions for misuse

- **I understand that I am responsible for my actions, both in and out of the School.**
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy, I will be subject

to disciplinary action in accordance with the school's Behaviour Policy.

6.6 Declaration

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. a mobile phone before or after school day
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

7. Review

All serious online safety incidents will be logged. The DSL will always consider whether external agencies should be informed such as BSCP or the Police.

The record of online safety incidents will be reviewed regularly to consider whether the existing systems and procedures are adequate.