



## **King Edward VI High School for Girls**

# **Pupils' Acceptable Use of ICT, Mobile Phones and Electronic Devices**

<b>Committee</b>	<b>N/A</b>
<b>Policy Type</b>	<b>School</b>
<b>Policy Owner</b>	<b>Vice Principal (Pastoral)</b>
<b>Statutory</b>	<b>No</b>
<b>Published on website</b>	<b>Yes</b>
<b>Last review date</b>	<b>07/2023</b>
<b>Next review date</b>	<b>07/2024</b>
<b>Review Cycle</b>	<b>Annual</b>
<b>Expiry date</b>	<b>N/A</b>
<b>Version</b>	<b>1.1</b>

## **PUPILS' ACCEPTABLE USE OF ICT, MOBILE PHONES AND ELECTRONIC DEVICES**

### **CONTENTS**

1. Introduction
2. Aim and scope of this policy
3. Promoting Safe Use of Technology and the Role of Staff
4. Involvement with Parents and Guardians
5. Acceptable Use Policy Agreement
  - 5.1 For my own personal safety and that of others
  - 5.2 For protection of pupils, others and the School
  - 5.3 Guidelines for use of personal mobile devices
  - 5.4 Searching electronic devices
  - 5.5 Reporting incidents of misuse
  - 5.6 Sanctions for misuse
  - 5.7 Acceptable Use Policy Agreement Form
6. Review

## **1. INTRODUCTION**

This policy relates to all pupils at KEHS and should be read in conjunction with the School's Behaviour and Discipline 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 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.

In general, our approach and expectations are guided by our school aims, which can be found on the school website.

The school provides its pupils with access to the school network and internet in order to enhance pupils' education and learning. The internet can offer great opportunities for learning, but also, of course, opportunities for misbehaviour 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 and sensitively when using computer equipment, mobile technologies or accessing the internet.

Digital learning is a component of every academic subject and is also taught as a subject in its own right. When available, pupils may use the machines in the ICT 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.

## **3. PROMOTING SAFE USE OF TECHNOLOGY AND THE ROLE OF STAFF**

Online safety training for staff is provided as part of our overarching approach to safeguarding children and staff reinforce e-safety messages across the curriculum. We aim to build resilience in our students to protect themselves and their peers through education and information.

Pupils in Year 7 complete a unit of work on Internet Safety, focusing on how to behave responsibly online, staying safe online 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, form time and assemblies as pupils progress through the school. 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 on-line through their use of social media, in keeping with the Prevent Duty.

Our Designated Safeguarding Lead (DSL) is aware of the safety issues involved with the misuse of the internet and other mobile electronic devices. 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 Digital Learning to ensure online safety education is mapped across the curriculum.

The DSL (Vice Principal Pastoral) monitors pupil use of the internet in School. It is the DSL's responsibility to handle allegations of misuse of the internet. The school network uses Smoothwall systems for filtering and active monitoring. Any required action following a student's inappropriate use of the network is recorded in CPOMS along with the support and guidance offered to the pupil to encourage more safe and responsible use in the future.

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.

#### **4. INVOLVEMENT WITH PARENTS AND GUARDIANS**

We seek to work closely with parents and guardians in promoting a culture of e-safety; we recognise that they play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. We will always contact parents if we have any worries about a student's behaviour in this area, and we encourage parents to share any worries they have with us.

We recognise that not all parents and guardians may feel equipped to protect their children when they use electronic equipment 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 help their children be discriminating, web-literate and resilient.

Parents are encouraged to support the school in promoting good e-safety practice and are asked to read the Pupils' Acceptable Use Policy with which all pupils must comply.

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.

#### **5. 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.

### **5.1 For my own personal safety and that of others:**

- I recognise that the school will actively monitor my use of school digital 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, gender, 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 Vice Principal (Pastoral).
- 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.

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

- I understand the risks and will not try to upload, download or access any internet sites which contain obscene, hateful or otherwise illegal material or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / monitoring/ security systems in place to prevent access to such materials.
- 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. I will not install or run any unauthorised form of software on the school network, nor will I introduce viruses.
- I will seek permission from a member of staff before attaching hardware such as USB keys into the school network.
- 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 from social networking sites.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

### 5.3 Guidelines for Use of Personal Mobile Devices

We believe it is important for our pupils to spend time interacting with one another, relaxing, or participating in extra-curricular activities at recess and lunch time. Whilst electronic devices are hugely beneficial in many respects, we do not consider their use during the school day to be necessary. Students are not permitted to wear Smart Watches, 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 8.30am until the end of the school day, unless a teacher has given permission for their use.** If there is an urgent need to contact a parent during these hours, then pupils must first seek permission from any member of staff; if permitted, the use will be supervised.

We support parents who make the decision that their child does not need to bring a mobile phone to school at all by ensuring that 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:

- Mobile phones and other personal devices must remain switched off and out of sight from 8.30am until the end of the school day whilst on school premises, unless a teacher has given permission for their use.
- Before 8.30am mobile phones may be used in the form room, or outside the buildings (away from car parks). No member of the school community should be disturbed by the use which must also comply with the points set out in sections 5.1 and 5.2 of the Pupils' AUP. After school mobile phones may be used, except in corridors.
- Mobile phones must not be seen or used in locker rooms, corridors, library or dining hall.
- Earphones or 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 form 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 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. Parents will of course be informed if necessary.
- Pupils may never use a mobile device to take photographs or make videos without the express permission of a teacher.
- Staff may confiscate mobile phones, where use has contravened the rules, until the end of that school day (though for more serious cases, confiscation may be for a longer period – see section 5.4). 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 brought onto school premises.
- In an emergency, common sense should prevail.

### **Sixth Form**

- Mobile phones should be switched off and out of sight during all lessons, assemblies and form time, unless a teacher has given permission for their use.
- 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 library, which means that calls cannot be made or taken there. All use must comply with the points set out in sections 5.1 and 5.2 with one exception: girls 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.
- Mobile phones, earphones and headphones must not be seen or used in locker rooms, corridors, form rooms or dining hall, unless a teacher has given permission for this.
- 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 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 at any time 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. Parents will of course be informed if necessary.
- Pupils may never use a mobile device to take photographs or make videos without the express permission of a teacher.

- Staff may confiscate mobile phones, where use has contravened the rules, until the end of that school day (though for more serious cases, confiscation may be for a longer period – see section 5.4). It is the student's responsibility to collect a confiscated device from Reception promptly at the end of the day.
- Repeated breach of these 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 brought onto school premises.
- In an emergency, common sense should prevail.

#### **5.4 Searching electronic devices**

If a member of staff has good reason to believe that a personal device has been used for sexting, 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](#).

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 Vice Principal (Pastoral) or Assistant Head (Pastoral) who will follow the DfE guidance: [Searching, Screening and Confiscation: advice for schools](#).

#### **5.5 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.

#### **5.6 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 and Discipline Policy.

## **5.7 ACCEPTABLE USE POLICY AGREEMENT FORM**

This form relates to the Acceptable Use Policy for Pupils, to which it is attached.

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. mobile phone
- 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.

**All pupils must confirm their acceptance of this agreement.**

## **6 REVIEW**

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

The record of e-safety incidents and new technologies will be reviewed regularly in order to consider whether the existing security procedures are adequate.