ONLINE SAFETY AND ACCEPTABLE USE POLICY (AUP)

Policy Name:	Online Safety and Acceptable Use Policy
Policy Type	Non-Statutory
Issue Date	16th January 2023
To Be Reviewed	Biannually – January 2025
Approved by Headteacher	Jennifer Giovanelli

Policy Statement

At Kingsthorpe College we are passionate about ensuring our students have the skills needed to thrive in an increasingly digital world. Safe and responsible use of the technology and the internet is therefore something we take very seriously. At present, the internet-based technologies used extensively by young people in both home and school environments include:

- Websites
- Social Media apps, including Instagram, SnapChat, and TikTok
- Web enabled mobile/smart phones
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Video broadcasting, including Chat Roulette, Omegle
- Vlogging apps such as YouTube
- Blogs and Wikis
- Email, forums, Instant Messaging and Chat Rooms

Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, safety, age restrictions and potential risks are crucial.

All schools have a duty to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks; however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people, and staff continue to be protected.

Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies (including all online technologies) both within, and outside of, the school environment.
- To educate staff, children and young people, parents and carers about the 4 C's or risks of online safety including **content**, **contact**, **conduct**, and **commerce**.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Scope of policy

This policy applies to all staff, students, governors, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or student use of personal devices, such as laptops, mobile phones or iPads which are brought onto school grounds. This policy is also applicable where staff have been provided with school issued devices for use off-site, such as school laptop or work mobile phone.

Staff Responsibilities

Teaching and Support Staff (including volunteers)

All staff have a shared responsibility to ensure that children and young people are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound.

Network Manager/Technical Staff

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and not open to misuse or malicious attack.
- that anti-virus software is installed and maintained on all school machines and portable devices.
- that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the Designated Safeguarding Lead (DSL).
- that any problems or faults relating to filtering are reported to DSL and to the broadband provider immediately and recorded on MyConcern.
- that staff may only access the school's network through a rigorously enforced password protection policy, in which passwords are regularly changed.
- that he/she keeps up to date with online safety technical information to maintain the security of the school network and safeguard children and young people.
- that the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the DSL and/or the Headteacher.

Children and Young People

Children and young people are responsible for:

- reading, agreeing to, and abiding by, the 'Acceptable Use Rules for Students'. These rules have been written to help keep everyone safe and happy when they are online or using technology.
- using the internet and technologies in a safe and responsible manner within school.
- informing staff of any illegal, inappropriate or harmful **content**, **contact** from unknown sources, **conduct** including cyberbullying, or **commerce** materials.
- via our Student Digital Leaders, actively participating in the development and biannual review of the Acceptable Use Policy.

We ask all children and young people at Kingsthorpe College to follow these steps to remember the 4 C's of online safety:

1. **Protect your online reputation**

   Use the services provided to manage your digital footprints and 'think before you post.' Content posted online can last forever and could be shared publicly by anyone.

2. **Know where to find help**

   Understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it's never too late to tell someone. Check our display beside Student Services which contains information about blocking and reporting incidents on all social media platforms.

3. **Don't give in to pressure**

   Keep calm and keep in control; once you've pressed send you can't take it back. Conduct yourself online as you would in the offline world.

4. **Respect the law**

   Use reliable services and know how to legally access the music, film and TV you want. Do not access, create or share illegal, inappropriate or harmful content.

5. **Acknowledge your sources**

   Use trustworthy content and remember to give credit when using others' work/ideas. Check you are not accessing inappropriate advertising, phishing and or financial scams.

Incident Reporting

In the event of misuse by staff or students, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Headteacher/IT Services Manager immediately. Incidents of Cyber Bullying should be reported in accordance with the School's Anti-Bullying Policy. MyConcern should be completed for all incidents involving students.

In the event of minor or accidental misuse, internal investigations should be initiated, and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of IT should be reported immediately to the IT Services Manager and/or Headteacher.

All incidents must be recorded on the IT Services Help Desk system, through the IT Services Manager, to allow for monitoring, auditing and identification of specific concerns or trends.

Monitoring

School ICT technical staff regularly monitor and record user activity, including any personal use of the school ICT system (both within and outside of the school environment). Monitoring software is installed on most computer equipment used in school, which logs such activity as websites visited, programs used, files printed, etc. Random reviews of these logs are undertaken to ensure that equipment is being used appropriately.

The Network Manager has the facility to access all files on the school network and to gain access to email accounts. Email will only ever be accessed with consent of the member of staff concerned or as directed by the Headteacher.

The Curriculum

The school strives to embed online safety into all areas of our curriculum and key online safeguarding messages are reinforced wherever IT is used in learning as follows:

- A thorough programme of skills and competencies are taught across KS3 and KS4 in our digital literacy and computing curricula to ensure that students are able to explore how online technologies can be used effectively, but in a safe and responsible manner.
- Students are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the digital literacy curriculum.
- Opportunities for informal discussions with students about online risks and strategies for protecting yourself online are built into our PSHE curriculum, to ensure that our students are armed with accurate information.
- 'Safer Internet Day' is celebrated annually at our school, raising the profile of online safety amongst staff and students. A permanent display in maintained and updated outside Student Services containing the appropriate steps needed to report and block abuse on all online platforms.
- Students, parents/carers and staff are signposted to national and local organisations for further support and advice relating to online safety issues. We post updates on Student Year Group Teams as well as updates via the Arbor Parent App.

Students with additional learning needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each student. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

Email Use

Staff

- The school provides all staff with a professional email account to use for all school related business, including communications with children, parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Under no circumstances will staff members engage in any personal communications (i.e. via Hotmail or Yahoo accounts) with current, recent former students or any minor outside of authorised school systems.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- Staff should inform their line manager or the IT Services team if they receive an offensive or inappropriate email via the school system.

Students

- The school provides individual email accounts for students to use as part of their entitlement to understand different ways of communicating and using ICT to share and present information.
- Students will use their school issued email account for any school related communications, including homework or correspondence with teachers. Email and Microsoft Teams chat content will be subject to monitoring and filtering for safeguarding purposes.
- Students will be taught about email safety issues, such as the risk of exposing personal information, opening attachments from unknown sources and the management of inappropriate emails. Students will also be guided in the correct tone to use in email correspondence and regularly reminded of restrictions on abusive or inappropriate content.
- The forwarding of chain letters is strictly prohibited in school and should be reported to a member of staff immediately.

Both

- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the Network Manager or Headteacher. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Headteacher and/or Network Manager.

Managing remote access

As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school network and email using remote access facilities.

For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Only equipment with the appropriate level of security should be used for remote access (i.e. up-to-date anti-virus should be installed and enabled; encryption on any devices where sensitive data is stored or accessed if possible).
- Log-on information should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns)
- For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.

Internet Access and Filtering

Broadband Provider: **EXA Networks**

All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Headteacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that internet filtering is in place to protect young users from inappropriate or harmful online content.

To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored in school via an administration tool/control panel, provided by **Lightspeed**, which allows an authorised staff member to instantly allow or block access to a site or specific pages and manage user internet access.
- Age-appropriate content filtering (including measures to ensure students are safe from terrorism and extremist material) is in place across the school, ensuring that staff and students receive different levels of filtered internet access in line with user requirements (e.g. YouTube at sixth form and staff level but blocked to main school students).
- All users have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering.

In addition to the above, the following safeguards are also in place:

- Anti-virus and anti-spyware software is used on all network and standalone PCs and laptops and is updated on a regular basis.
- A firewall is in place to protect the school network and the information about children and young people it contains from access by unauthorised users. The firewall is routinely patched to prevent new and emerging security risks.
- Encryption codes on wireless systems prevent unauthorised use.
- A link to The Child Exploitation and Online Protection (CEOP) Report Abuse button is available via the school website to allow students or staff to report online safeguarding issues.
- All staff at Kingsthorpe College have annual Prevent training and have a duty to be vigilant and report any concerns over use of the internet that includes, for example, attempted internet searches related to extremism, attempted visits to extremist websites, attempted use of social media to read or post extremist material, online grooming of individuals.

Staff

- Expectations for staff online conduct are the same professional expectations as those offline and are detailed in the staff code of conduct.
- Staff are expected to preview any websites before use, including those which are recommended to students and parents for homework support.

Use of School and Personal ICT Equipment

School ICT Equipment

- A log of all ICT equipment issued to staff, including serial numbers, is maintained and held by the Network Manager.
- Staff should ensure that equipment is secured when not in use (e.g. locking workstations when leaving rooms and ensuring that laptops are returned to locked cupboards when no longer needed).
- Devices owned by the school are loaned to staff members as required by their duties, on the understanding that they are treated with care and looked after responsibly. Ownership of any such device remains with the school.

- Loss or damage to school equipment should be reported immediately to the Network Manager.
- All data residing on the school network or devices owned by the school is the property of Kingsthorpe College.
- Personal data, such as digital photographs and music, should not be stored on school equipment, and may be subject to periodic deletion as part of our monitoring processes.
- Whilst the school performs backups of data residing on our systems, we are not responsible for the loss of such data.
- Personal ICT equipment, such as laptops or memory sticks, must not be connected to the school network without consent from the Network Manager and a thorough virus check.

Mobile/Smart Phones

Student use:

- Sixth form students are permitted mobile phones/devices in school for responsible use outside of lesson times, subject to the mobile phone policy currently in place. Misuse of mobile devices on school grounds will result in the loss of this privilege.
- Students in years 7-11 are not permitted to use their mobile phones in school, unless part of a planned educational activity and under direction of their teacher. Mobile phones are not allowed at any other time.
- If there is reason to suspect that a student's mobile device contains inappropriate, harmful or illegal content, the device will be confiscated, and a search conducted by a member of the SLT in line with disciplinary powers awarded to staff in the Education Act 2011. Searches will be conducted in the presence of at least one other SLT member and any actions/findings (including contacting the relevant authorities) and logged on MyConcern. Where evidence of illegal activity is discovered (e.g. indecent images of young people) the device will be locked in a secure area, parents/carers will be notified and the police contacted immediately.

Staff use:

Personal mobile phones are permitted on school grounds but should be used outside of lesson time only.

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile phones should never be used to contact students or their families, or to take photos or videos of students.

Laptops/ iPads

- Personal use of school laptops or computing facilities, whilst on site, is left to the discretion of the Headteacher and may be permissible if kept to a minimum, used outside of lesson times and does not interfere with an employee's work.
- Some staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members).

- Software and apps should not be installed on school owned devices without prior permission of the Network Manager. Restrictions are usually in place to prevent this, as the school has a duty to ensure software is licensed appropriately.
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti- virus updates, software installations, patches, upgrades, or routine monitoring/servicing.

Removable Media (Memory Sticks/USB)

- Where staff may require removable media to store or access sensitive data (e.g. IEPs, student attainment and assessment data) off site, this use should be kept as minimal as possible to restrict the chance of loss. The use of encrypted memory sticks is strongly recommended.
- Any passwords used for encrypted memory sticks/or other devices will remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

Photographs and Video

Digital photographs and videos are an important part of the learning experience for children and young people and, as such, schools have a responsibility to ensure that they not only educate students about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and students about the use of digital imagery within school.

- Written consent will be obtained from parents or carers before photographs or videos of students will be taken or used within the school environment, including the school website or associated marketing material.
- Permission will be sought from any student or staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.
- Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Headteacher for use of personal equipment for school related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device. This permission must be in writing for audit purposes.
- Where photographs of students are published or displayed (e.g. on the school website) parental consent must be received.
- Wherever possible, group shots of students will be taken, as opposed to images of individuals and images should never show young people in compromising situations or inappropriate clothing.

Social Networks

Staff must take care when using social networking websites such as Facebook, Instagram, or Twitter, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children. Current advice is to change your name on social network sites (e.g. using your middle name instead of surname), making it harder for students to find your account. Friends and family could be told your alias, enabling them to still make contact.

You must not allow any student to access personal information you post on a social networking site. In particular:

- You **must not** add a student to your 'friends list' or be 'following' them.
- You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- You should **avoid** contacting any student privately via a social networking website, even for school-related purposes.
- You should **take steps** to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff or a student, that could potentially be used to embarrass, harass, or defame the subject.

Any concerns, including those about another person, should be raised with the DSL. For further advice, staff are advised to speak to either the IT services team or their union.

Video conferencing

- Permission must be obtained from parents and carers prior to their child's involvement in video conferencing.
- All students must be supervised by a member of staff when video conferencing, particularly when communicating with individuals or groups outside of the school environment (e.g. international schools)
- All video conferencing activities must be time logged and dated with a list of participants.

Parent / Carer Involvement

As part of the school's commitment to developing online safety awareness amongst children and young people, every effort is made to engage parents and carers in the process.

- All students and their parents/carers will receive a copy of the Acceptable Use Rules (Appendix A) on an annual basis or first-time entry to the school. Students and their parents/carers are both asked to read and digest the rules, a copy of which will be stored at school. Any questions or non-acceptance should be directed to the school office.
- Parents/carers are encouraged to visit sites such as those listed below to research online safety materials and resources. Our school website contains an online safety page with other useful links and advice.
    - support for parents and carers to keep children safe from online harm which provides extensive resources to help keep children safe online and details of specific online risks, including sexual abuse, criminal exploitation and radicalisation.
    - CEOP Education provides advice from the NCA on staying safe online.
    - Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support.
    - Internet matters provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world.
    - London Grid for Learning (LGfL) has support for parents and carers to keep their children safe online.
    - Keeping children safe online has support for parents and carers from the NSPCC, including guides on social media, internet connected devices and toys and online games.
    - Let's Talk About It has advice for parents and carers to keep children safe from online radicalisation.
    - UK Safer Internet Centre has tips, advice, guides, and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services.
- Regular online safety tips, advice and updates are sent to parents/carers via the Arbor Parent App.

Appendix A: Student and Parent/Carer AUP and Online Safety Agreements

I know that I must use the computers safely:

- I understand that I am forbidden to use any technology designed to avoid or bypass school filtering controls. We know that these filters are in place to protect us from viewing websites that are unsuitable or unsafe for us.
- I know that the school can remotely monitor what I do on the computers.
- I will treat my username and password like my toothbrush – I will not let anyone else use it and I will not use theirs.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer or anything that makes me feel uncomfortable or unsafe when I see it.
- I will not ever provide personal information about myself and anyone else, such as my address, telephone number and private details in an email or on a website. I know I could put myself and/or others in danger.
- I know that I can go to Think U Know for further help or use the display board outside Student Services to find tips about blocking, removing, and reporting content, cyberbullying or unwanted or harmful contact.

I know that I must use the computers responsibly:

- I understand that the computers are provided to support learning only.
- I understand that the school's security and internet filter is there to protect me and protect the computer network and I will not try to bypass it. If I need access to a blocked website, I will ask my teacher.
- I will only download music or videos onto the computer if it is related to my schoolwork and with permission from my teacher.
- I understand that I must not download or display inappropriate pictures or other material from the Internet.
- I do not assume that information published on the Internet or written in an e-mail is accurate, true, or unbiased.
- When using email or Teams chat, I will only write to people approved by our teacher in college.
- I am careful about what I write. I check my work before I print or send anything. I do not use inappropriate language. I do not write racist, sexist, abusive, homophobic, transphobic, or aggressive words. I do not write anything that could upset and offend others.
- I will not access sites or download any materials, which are illegal, promote terrorism or extremism, are offensive, violent and/or pornographic in nature.

I know that I must help look after the computers:

- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I won't leave it broken for the next person.
- I will only use programs that are already on the school computer.
- I will not try to connect my own computer or mobile phone to the network.
- I know that food and drink is not allowed in the computer rooms and that I should not

eat or drink around any computer.

I know that I must respect others when using the computers:

- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass, abuse, offend or bully anyone.
- I will be polite online, and I will not use strong, aggressive, offensive, sexualised or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.
- I will not access, create or display any material (e.g. images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to myself and others.
- I always respect the privacy of other users' files.
- I will report any incident that breaches the Acceptable Use Policy rules immediately to my teacher.
- I understand that any breach of the Acceptable Use Policy may incur consequences under the Policy.

STUDENT ONLINE SAFETY AGREEMENTS

Student

- I agree to comply with the college rules on the responsible use of IT. I will use the college network in a responsible way, and I understand the sanctions for breaking these rules.
- I have read, understood, and agree with the above acceptable use rules for the use of the internet at school.

Parent/Carer

- As the parent/legal carer of Kingsthorpe College student I grant the permission for my child to use the Internet, school email account and Microsoft Teams.
- I understand that students will be held accountable for their actions and that the rules/sanctions have been explained.
- I understand that whilst every reasonable endeavour is made to ensure that suitable precautions are taken, the college cannot guarantee that students do not see undesirable material.

PARENT/CARER ONLINE SAFETY AGREEMENTS

- I understand that Kingsthorpe College uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
- I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
- I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, including during any remote learning periods.
- I will promote positive online safety and model safe, responsible, and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media acceptable use guidance and not encourage my child to join any platform where they are below the minimum age.
- I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
- I understand that for my child to grow up safe online, they will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism, terrorism, gangs, sharing inappropriate content etc.
- I understand that my child needs a safe and appropriate place to do remote learning if the College or Year Groups are closed. When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
- I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.

- I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 a Day.
- I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which they have signed, and which can be found in Appendix A, and I understand that they will be subject to sanctions if they do not follow these rules.
- I can talk to my child/ren's tutor or Head of Year, if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood, and agreed to this policy.

Appendix B– Post 16 Device and Internet Access Policy

Objectives and Agreements

At Kingsthorpe College Post 16 students may bring their own personal computing devices (including but not limited to, the following that is owned by the student: laptop computer, netbook, tablets, e-reader, iOS and Android based devices) and are allowed to connect to the school's wireless network. The Acceptable Use Policy guidelines apply when using personal computing devices such as laptops, mobile phones and tablets at school. In addition to following the policy all students must agree to the following terms.

- I will connect to the school's wireless network, and NOT to the school's wired network, or any visible network in the neighbourhood.
- In class, I will use the device only for educational activities with the teacher's expressed permission.
- I understand that taking pictures and/or recording videos and audios of my peers and/or staff in school for personal use without permission constitutes a breach of the Acceptable Use Policy.
- The device I am using will have virus protection software which is up to date.
- I will turn off all peer-to-peer (music, video and/or file-sharing) software or web-hosting services on my device while connected to the school's wireless network.
- I will NOT use the school's wireless network for downloading videos, music, games or other large files for my personal use.
- I understand that the school is not responsible for the loss, theft, damage, use or maintenance of my device. I am fully responsible for my property.
- I understand that Kingsthorpe College may access my personal computing device if there are reasonable grounds to believe that there has been a breach of the college's Acceptable Use Policy and that a search of the device would reveal evidence of that breach. This may include, but is not limited to, audio and video recording, photographs taken on school property that violate the privacy of others, as well as in relation bullying, etc.

Post 16 Student IT use at Kingsthorpe College

At Kingsthorpe College, students are allowed access to our curriculum network and the Internet including remote learning platforms such as Microsoft365, enabling them to use a wide variety of resources and communicate effectively with both teachers and peers, in support of research and education. They are also encouraged to be aware of the safety rules and procedures which regulate our use of the technology, the Internet and Microsoft365.

- I understand that these facilities must be used for educational purposes and in an appropriate manner. I know that any breach of the rules will be considered a disciplinary matter.
- I must have permission from our parents/carers before I can use the internet for independent research at college.
- I know that access to the networked resources is a privilege. I am encouraged to make use of the Internet in support of my studies in all subjects.

- I do not access, create or display any material (e.g. images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to ourselves and others.
- I do not assume that information published on the Internet or written in an e-mail is accurate, unbiased or true.
- I keep my username and password private. I do not tell anyone.
- When I use email and Teams chat, I only write to people approved by my teacher in college.
- I am careful about what I write. I check my work before I print or send anything. I do not use inappropriate language. I do not write racist, sexist, abusive, homophobic, transphobic, or aggressive words. I do not write anything that could upset and offend others.
- I will not access sites or download any materials, which are illegal, promote terrorism or extremism, are offensive, violent and/or pornographic in nature.
- I will not ever provide personal information about myself and anyone else, such as our address, telephone number and private details in an email or on a website. I know I could put myself and/or others in danger.
- I do not respond to suspicious e-mail messages. I let our teachers know immediately if I am sent anything we do not feel comfortable with.
- I understand that I am forbidden to use any technology designed to avoid or bypass school filtering controls. I know that these filters are in place to protect me from viewing websites that are unsuitable or unsafe for me.
- I always respect the privacy of other users' files.
- I will report any incident that breaches the Acceptable Use Policy rules immediately to our teacher.
- I understand that any breach of the Acceptable Use Policy may incur consequences under the Policy.
- I know that we can go to Think U Know for further help.

Kingsthorpe College's ISP operates a filtering system in line with LA requirements, which restricts access to inappropriate websites; students must also be supervised when using the computers. However, it is impossible to guarantee that the supervision and filtering system will prevent students accessing undesirable material.

POST 16 ONLINE SAFETY AGREEMENTS AND AUP

Student

- I agree to comply with the college rules on the responsible use of ICT. I will use the college network in a responsible way, and I understand the sanctions for breaking these rules.
- I have read, understood, and agree with the above rules for the use of personal computing devices at school.
- I accept all responsibility when bringing my own personal computing device to school.

Parent

- As the parent/legal guardian of the above student I grant the permission for my child to use the Internet and Email.
- I understand that students will be held accountable for their actions and that the rules/sanctions have been explained.
- I understand that whilst every reasonable endeavour is made to ensure that suitable precautions are taken, the college cannot guarantee that students do not see undesirable material.
- I have reviewed all expectations with my child about bringing in their own personal device.
- My child understands the expectations and responsibilities associated with using personal computing devices at school.
- I hereby release Kingsthorpe College and its personnel from any and all claims and damages arising from my child's use of, or inability to use, their personal wireless device on the college's wireless network.
- I give permission to allow my child to bring their personal computing device to school for educational use.