Kings International College

E-Safety Policy

`

Contents

Policy Objectives 2

General Statement 2

The Internet 2

Managing Internet Access to ensure security and confidentiality 3

Communicating the E-Safety Policy to students, staff and parents 5

Roles and Responsibilities 6

Behaviour 8

The Law 9

Appendix 1 10

Appendix 2 11

Appendix 3 13

Approved by:	FGB	**Date:**	20.6.19
Status and Review Cycle			
Person(s) responsible	AIN		
Last reviewed on:	20.6.19		
Next review due by:			Summer 2021

Policy Objectives

•To provide high quality and safe internet access for all students and staff

•To promote and secure the welfare of all students through clear communication of expectation, protocol and procedure for all users of ICT

•To rigorously monitor and review ICT use and practice by all

•To teach and communicate to students what internet use is acceptable and what is not and give clear expectations for Internet use

•To educate all students in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

•To ensure that the use of Internet derived materials by staff and by students complies with copyright law.

•To make explicit to students and staff the procedures for reporting inappropriate and offensive Internet and ICT content e.g. using the CEOP Report Abuse icon or Hector Protector.

General Statement

Kings International College recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement safeguards within the school and to support staff and students to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies.

In our duty to safeguard students we will do all that we can to make our students and staff stay e-safe and to satisfy our wider duty of care. This E-safety policy should be read in conjunction with other relevant school policies, including Safeguarding Students: Child Protection. Behaviour Policy and the Anti-bullying policy.

The policy applies to all students, staff and all members of the school community who have access to the school IT systems, both on the premises and remotely. Any user of the school IT systems must adhere to and sign a hard copy of the e-Safety Rules and the Acceptable Use Agreement. The E-safety Policy applies to all use of the internet and electronic communication devices such as email, mobile phones, games consoles and social networking sites.

The Internet

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and students. This policy will provide guidance on the usage of ICT for students and staff.

Managing Internet Access to ensure security and confidentiality

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority and local schools.

E-mail

- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to student email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or student personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual students. See use of images policy for additional information.
- Students' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- The school will control access to social networking sites, and consider how to educate students in their safe use e.g. use of passwords.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must not place personal photos on any social network space provided in the school learning platform.
- Students and parents will be advised that the use of social network spaces outside school brings a range of dangers.
- Students will be advised to use nicknames and avatars when using social networking sites.

- Staff will be advised on the appropriate use of social networking with students. If staff are networking with students, they will be advised to use a professional login and keep their personal users separate.

Managing filtering

- The school will work to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, the site must be reported to the IT systems manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of a staff sanctioned educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school if used by staff during lessons.
- Staff will use a school phone where contact with students is required. The appropriate use of Learning Platforms will be discussed as the technology progresses Protecting personal data
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

- All staff must read and sign the ICT code of conduct before using any school ICT resource.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with in the first instance by the E-safety Coordinator who will liaise directly with Senior Staff.
- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Students and parents will be informed of consequences for students misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communicating the E-Safety Policy to students, staff and parents

Introducing the E-safety policy to students

- Appropriate elements of the E-safety policy will be shared with students
- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for students

Staff and the E-safety policy

- All staff will be given the School E-safety Policy with its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /student agreement when they register their child with the school.

Roles and Responsibilities

There are clear lines of responsibility for E-safety within the school. The first point of contact for staff should be the E-safety Coordinator, who will then communicate issues of concern to the DSL or DDSL's where deemed appropriate to do so.

- All staff are responsible for ensuring the safety of students and should report any concerns immediately to their subject leader and the E-safety Coordinator.
- Teaching staff are required to deliver E-safety lessons to classes. This will be via IT lessons or tutorials / assemblies.
- When informed about an E-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.
- All students must know what to do if they have E-safety concerns and who to talk to. In most cases, this will be their teacher, Year Leader or E-safety coordinator in the first instance.
- Where any report of an E-safety incident is made, all parties should know what procedure is triggered and how this will be followed up.
- Where the E-safety Coordinator considers it appropriate with a student at possible serious risk, the Child Protection Liaison Officer will be asked to intervene with appropriate additional support from external agencies.

E-Safety Coordinator: (ESC)

The E-safety Coordinator is responsible for leading the E-safety Committee, leading policy review, delivering staff development and training, recording incidents, reporting any developments and incidents to the E-safety Safeguarding Officer and liaising with the local authority and external agencies to promote E-safety within the school community. He/she may also be required to deliver workshops for parents.

E-Safety Safeguarding Officer: (ESSO)

The E-Safety Safeguarding Officer, a member of the Senior Leadership Team, will action and sanction students resulting from serious incidents of ICT/internet misuse as reported by, and in liaison with, the E-safety Coordinator. He/she will also be responsible for communicating with the police, parents, the DSL, the Headteacher and outside agencies as appropriate in addressing such incidents.

Students:

Students are responsible for using the school ICT systems and mobile devices in accordance with the school Acceptable Use Policy and the E-safety Rules, which they must agree to and sign. Students are responsible for attending e-safety lessons as part of the curriculum. They are expected to seek help and follow procedures where they are worried or concerned, or where they believe an E-safety incident has taken place involving them or another member of the school community. Students must act safely and responsibly at all times when using the internet and/or mobile technologies.

Staff:

All staff are responsible for using the school ICT systems and mobile devices in accordance with the school Acceptable Use Policy and the E-safety Rules, which they must actively promote through embedded good practice. Staff are responsible for attending staff training on E-safety and displaying a model example to students at all times. All digital communications with students must be

professional in tone and content at all times. Online communication with students is restricted and must only be done through the school network or the VLE. All staff should apply relevant school policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the E-safety Coordinator and subject leader without delay.

Governors:

The link governor will hold the school accountable for monitoring and reporting practice in line with the E-Safety policy, reporting to the Full Governing Body (FGB).

Positions of Responsibility at date of policy review:

Subject Leader for ICT – Keith Price

E-Safety Safeguarding Officer – Alan Inns

Designated Safeguard Lead – Alan Inns

ICT Network Manager – Chris Dickson

ICT link governor - Susan Belgrave

Safeguarding link governor – David Barter

Behaviour

Kings International College will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy. The school will not tolerate any abuse of ICT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police. This includes incidents of cyberbullying.

Sanctions (see appendix 4)

The school will take all reasonable precautions to ensure E-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Staff and students are given information about infringements in use and sanctions. Sanctions include:

- Interview, counselling and/or disciplinary action by the teacher, Subject Leader Year Leader, E-safety Coordinator, E-safety Safeguarding Officer or Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- Referral to LA / Police
- Internal and external exclusion

The E-safety Coordinator will act as first point of contact for any complaint, in the first instance, reporting to the E-safety Safeguarding Officer as deemed appropriate. Any complaint about staff misuse will be referred to the Headteacher and may result in formal disciplinary proceedings. Complaints of cyber-bullying are dealt with in accordance with the school's Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school policy Safeguarding Students: Child Protection and LA child protection procedures.

Monitoring, Review and Impact

The impact of the policy will be monitored regularly with a full review being carried out at annually, undertaken by the E-Safety Coordinator and the E-safety Committee, senior leadership team, Safeguarding Strategic Group, link governor for ICT, staff and students. In the event that any concerns are raised in the interim, triggered by incidents or unforeseen circumstances, the review of policy will be brought forward.

The Law

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he/she knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Computer Misuse Act 1990

This legislation makes it a criminal offence to gain unauthorised access to another students area even if you don’t change/delete any information on the area.

Appendix 1

Staff, Governor and Visitors ICT Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life at Kings International College. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this code of conduct and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr Inns, Assistant Headteacher. In addition please ensure that you are familiar with the full ICT E-Safety policy, available on the staff shared drive: T:\College Management\Policies

- I will only use the school's email and Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- If transferring data physically off site I will do so using a school encrypted USB drive.
- Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. This is in line with the data protection policy.
- I will not install any hardware or software without permission of the IT Manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher. Images will only be taken with school equipment.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name …….. (Printed)

Appendix 2

E-safety Rules

These E-safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- I understand the school owns the computer network and learning platform and can set rules for its use. I understand it is a criminal offence to use a computer or network for a purpose not permitted by the school.
- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes. I will not use ICT systems at school for private purposes, unless the Headteacher has given specific permission.
- I will not use ICT systems at school for personal financial gain, gambling, political activity, advertising or illegal purposes.
- I will only log on to the school network/ learning platform with my own user name and password.
- I accept that I am responsible for all activity carried out under my username.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible, particularly as email could be forwarded to unintended readers.
- I will not send anonymous messages or chain mail.
- I will be responsible for my behaviour when using the Internet/learning platform. This includes resources I access and the language I use.
- I will be polite and appreciate that other users might have different views to my own.
- I will use the discussion forums on the school's learning platform for exchanging information and will share my ideas constructively.
- I will not give out any personal information such as name, phone number or address through email, personal publishing, blogs, messaging or when using the school's learning platform. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not download or install software on school technologies.
- I will not attempt to bypass the Internet filtering system.

- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress.

- I will respect the privacy and ownership of others' work on-line at all times.

- I understand the school can exercise its right to monitor the use of the school's computer systems and learning platform, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

- I understand that all my use of the Internet, school's learning platform and other related technologies can therefore be monitored and logged and can be made available to my teachers.

- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted. I understand that irresponsible use may result in the loss of my network or Internet access.

I agree to follow the E-safety rules and to support the safe and responsible use of ICT at Kings International College

Student Signature……

Form …… Date…….

Appendix 3

E-safety Parental Consent Form

Kings International College

Parent/Carer consent form and E-safety Rules

All students use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign agreements to show that the E-safety Rules have been understood and agreed.

Parent / Carer name: ……

Student name: ……..…….

As the parent or legal guardian of the above student, I have read and understood the attached school E-safety rules and grant permission for my daughter or son to have access to use the Internet, school email system, learning platform and other ICT facilities at school.

I know that my daughter or son has signed an E-safety agreement form and that they have a copy of the school E-safety rules. We have discussed this document and my daughter or son agrees to follow the E-safety rules and to support the safe and responsible use of ICT at Kings International College.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching E-safety skills to students.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their E-safety or e-behaviour that they will contact me.

I understand the school is not liable for any damages arising from my child's use of the Internet facilities.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's E-safety.

Parent/Guardian signature: ……..

Date: ……

Further information for parents on E-safety can be found at:
http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/

Please complete, sign and return to the school secretary.

Appendix 4

E-safety sanctions

It is appropriate for people to be allowed a great deal of freedom in using ICT for study, work and leisure. With freedom comes responsibility. Kings International College cannot control what people, all over the world, make available on the Internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form. If material is considered to be unacceptable by the school when presented in a book, magazine, video, audio tape or spoken form, then it is not acceptable on the ICT network.

We expect all ICT users to take responsibility in the following ways:

Not to access or even try to access any material which is:

- Violent or that which glorifies violence
- Criminal, terrorist or glorified criminal activity (including drug abuse)
- Racist or designed to incite racial hatred
- Of extreme political opinion
- Pornographic or with otherwise unsuitable sexual content
- Crude, profane or with otherwise unsuitable language
- Blasphemous or mocking of religious and moral beliefs and values
- In breach of the law, including copyright law, data protection, and computer misuse
- Belongs to other users of ICT systems and which they do not have explicit permission to use
- Not to search for, or use websites that bypass the school's Internet filtering
- Not to download or even try to download any software without the explicit permission of a member of the ICT systems support department
- Not to attempt to install unauthorised and unlicensed software
- To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers
- Not to use other people's user ID or password, even with their permission
- Not to interfere with or cause malicious damage to the ICT Facilities
- To report any breach (deliberate or accidental) of this policy to Subject Leader of ICT immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Kings International College the right to access all material stored on its ICT system, including that held in personal areas of staff and student accounts for purposes of ensuring DFE, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the ICT facilities. Kings International College will act strongly against anyone whose use of ICT risks bringing the school into disrepute or risk the proper work of other users. Persistent offenders will be denied access to the ICT facilities – on a permanent basis.

Sanctions for the misuse of Kings International College facilities

First Offence

- The student will have a meeting with the E-safety Co-ordinator to discuss the breaking of the ICT AUP.
- The student may have restrictions placed on their use of the ICT facilities by the removing of email and/or Internet access for a minimum of one weeks.
- The student will need to read the ICT AUP to ensure they are clear about the regulations by the completion of an educational worksheet.
- The E-safety Co-ordinator will write a letter to parents (or phone if required) to inform them of the breaking of the ICT AUP.
- The student may receive a further sanction depending on the nature of the offence.
- The form tutor, Year Leader and E-safety Safeguarding Officer will be informed
- Second Offence
- The E-safety Safeguarding Officer will write a letter to parents and phone them to inform them of the breaking of the ICT AUP for the second time. The letter may include specific information about the offence.
- The student will have restrictions placed on their use of the ICT facilities by the removing of email and/or Internet access for a minimum of two weeks.
- The student may receive a further sanction depending on the nature of the offence.
- The form tutor, Year Leader and Headteacher will be informed

Third Offence

- The student will have their email and/or Internet access removed immediately by the E-safety Co-ordinator for a minimum of 4 weeks.
- The E-safety Safeguarding Officer will write a letter to parents and phone them to inform them of the breaking of the ICT AUP for the third time. Parents will be asked to come into school to discuss the breaking of the ICT AUP with the E-safety Co-ordinator, E-Safety Safeguarding Officer and Year Leader.
- The form tutor, Year Leader and Headteacher will be informed

Fourth Offence

- The student will have all access the school network removed immediately.
- The student will be banned from entering any ICT suite in the school unless accompanied by a teacher.
- The E-safety Safeguarding Officer will write a letter to parents and phone them to inform them of the breaking of the ICT AUP for the fourth time.
- The student and parents will have a meeting with the E-safety Co-ordinator, E- Safety Safeguarding Officer and Headteacher to discuss the breaking of the ICT AUP and the subsequent sanction which may involve a form of exclusion.

It should be noted that if a student puts themselves, other students or a member of staff in danger by giving out personal details they will be banned from using the ICT facilities for a fixed period of time and if required the police will be informed.