Kuwait International English School

E-Safety & Acceptable Use of IT Policy

Rationale

The use of information technologies and IT media has become integral to everyday life in modern society. At KIES, we use IT on a daily basis to enhance student learning in many diverse ways, both directly and indirectly. As a school, our role is not only to use and to teach our students to use these technologies, but also to educate the members of our community in how to use them safely and appropriately.

The purpose of this Policy is to:

- safeguard all students and staff;
- provide guidance for students, staff and parents on the appropriate use of information technologies and media;
- provide a balance to support innovation within a framework of good practice;
- prevent or address potential inappropriate use of social media and social networking sites;
- protect the school from legal risks and ensure that the reputation of the school and it's staff is protected.

E-Safety Principles

All members of the KIES community, whether they are using IT in school, at home or at any other workplace should:

- keep in mind that information on the Internet, including what is said, may not be true.
  If a student is unsure about something, they should check it with a member of staff.
- avoid sharing personal information, such as passwords and full names and addresses on the Internet.
  Students should avoid talking to anyone they do not know through chat sites, message boards, emails, etc. unless permission is given from a member of staff.
- should not share material such as pictures, writing, videos and sound recordings that will upset, worry or embarrass another person.
  A student should inform a teacher or parent if something upsets them or if they know of someone who is being bullied online.

Digital Citizenship

We define **Digital Citizenship** as:

The right for all members of the KIES community to use the internet and devices in a safe, responsible and legal way.

We commit to:

1. Creating a safe environment for students to learn online in school.
2. Raising awareness of social media issues, how to deal with these and how to make good *choices* when using technology in and beyond the classroom.
3. Using technology wisely and effectively to transform and enhance learning, not as a direct tool to substitute during tasks.

We cover Digital Citizenship through:

- Assemblies
- PSHE
- E-Safety Displays at school
- Tutor presentations
- Articles to parents
- International Celebration Days (Anti-Bullying week, etc.)
- Parent Information sessions
- ICT lessons

Acceptable Use of IT

Acceptable Use helps to ensure that students and staff can use various technologies, the Internet and e-mail at KIES in safety and security. It extends to out-of-school practice to help ensure that members of the KIES community are not knowingly subject to identify theft and fraud. It also helps KIES students to avoid cyber-bullying or becoming a victim of abuse. However, whilst we do all we can to reduce the risks associated with using the Internet, given its dynamic nature, no organization can guarantee that their system is 100% safe. Therefore, constant co-operation and vigilance is expected from everyone.

Acceptable Use highlights the 'personal responsibility' of every computer user at KIES, whether for drafting coursework on a word-processor or using the Internet for research. As a member of KIES, each student has a responsibility to inform a member of staff of any misuse of the network or other ICT facilities and every staff member has a responsibility to inform the IT Manager. Such misuse may come in many forms and will include anything sent of received that may cause offence to another student or to a member of staff.

Key responsibilities of the management team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the online safety (e-Safety) lead in the development of an online safety culture within the setting.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviour.
- Making appropriate resources available to support the development of an online safety culture. Taking responsibility for online safety incidents and liaising with external agencies as appropriate. Receiving and regularly reviewing online safety incident logs and

using them to inform and shape future practice. Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of school systems and networks.

Key responsibilities of the designated safeguarding/online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends. Coordinating participation in local and national events to promote positive online behaviour.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitor Internet filtering reports to identify behaviour which might indicate safeguarding issues or inappropriate behaviours.
- Update safeguarding log or e-safety incident log as appropriate.
- Monitor the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures. Meet regularly with the governor/board/committee member with a lead responsibility for online safety.

Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading and signing the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible. Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate online safety issues, internally and externally. Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

Additional responsibilities for the IT Manager are:

- Provide a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Take responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensure that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensure that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
- Develop an understanding of relevant legislation as it relates to security and safety of the technical infrastructure.
- Report any breaches and liaise with United Learning Technology Team (or other local or national bodies) as appropriate on technical infrastructure issues.
- Configure internet filters to generate regular safeguarding reports, as determined by e-safety leads, Progress team leads and DSL, and send to appropriate staff.
- Provide technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensure that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensure that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

Key responsibilities of children and young people are:

- Contributing to the development of online safety policies. Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult and supporting others when there are online safety issues.
- At a level that is appropriate to their individual age, ability and vulnerabilities:
    - Taking responsibility for keeping themselves and others safe online.
    - Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
    - Assessing personal risks of using a particular technology, and behaving safely and responsibly to limit risks.

Key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school/setting online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

All users must sign that they have read and understood what is meant by Acceptable Use and the expectations and responsibilities that this entails, as set out above. Failure to uphold this Acceptance Use Agreement may lead to loss of access to the school network and Internet or to other actions in accordance with the Positive Behaviour Policy and the Staff Code of Conduct.

Online Communication and Safer Use of Technology

Managing the school/setting website

- The school will ensure that information posted on the school website meets the requirements as identified by the Ministry of Education.
- The contact details on the website will be the school address, email and telephone number. Staff or students' personal information will not be published.
- The school website will comply with Ministry of Education's and the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- The school will post information about safeguarding, including online safety on the school website, or link to the resources hosted by Orbital education.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- Students' work will only be published with their permission or that of their parents/carers (Although this may be generic rather than item by item).

Publishing images and videos online

- The school will ensure that all images are used in accordance with the school image use policy.
- In line with the school's image policy, written permission from parents or carers will always be obtained before images/videos of students are electronically published via this form: https://form.jotform.com/223131042920440
- Any images, videos or music posted online will comply with the intellectual property rights and copyright

Managing email

- Students may only use school/setting provided email accounts for educational purposes.
- All members of staff are provided with a specific school/setting email address to use for any official communication. The use of personal email addresses by staff for any official school/setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Caution should be taken on opening emails with attachments or clicking on links within; being conscious of the risks from malware.
- Access in school to external personal email accounts may be blocked. Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The school will have a dedicated system for reporting safeguarding issues.
- This will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

- **E-mail and Mobile Phones**
- All e-mail communication between staff and members of the school community on school business must be made from an official school e-mail account.
- Staff members must be conscious at all times of the need to keep personal and professional lives separate and to always maintain appropriate professional boundaries. Staff should not use personal email accounts or personal mobile phones to make contact with students, nor should any such contact be accepted, except in circumstances given prior approval by the Principal. In the case of school trips, staff should make it clear when completing risk assessments that they will require student contact numbers. Student contact details must be deleted after the trip.

Appropriate and safe classroom use of the internet and associated devices

- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- Students will use age and ability appropriate tools to search the Internet for content. Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.
- The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use are essential.
- Supervision of students will be appropriate to their age and ability.
    - Secondary students will be appropriately supervised when using technology, according to their ability and understanding.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Mobile device management solutions will be used to record/enforce the rules of

the AUP.

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of online.materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

Management of school learning platforms/portals/gateways (LP)

- SLT and staff will regularly monitor the usage of the LP by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current student, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, students etc. leave the school their account or rights to specific school areas will be disabled and/or transferred to their new establishment as soon as possible.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
    - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    - b) The material will be removed by the site administrator if the user does not comply.
    - c) Access to the LP for the user may be suspended.
    - d) The user will need to discuss the issues with a member of leadership before reinstatement.
    - e) A student's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the leadership team. In this instance there may be an agreed focus or a limited time slot. Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

Mobile Technologies

The development and widespread use of tablets, smart phones and other devices has significantly changed the technology landscape. Mobile devices can be useful in many educational contexts, such as recording a student's own work through images or audio files or in the use of electronic calendars to plan work. In terms of teaching and learning they may be useful for e-mailing work home, researching on the internet, listening to revision podcasts, or as electronic dictionaries. As a school, Secondary students are all expected to use the school ICT facilities.

Additionally, many parents consider mobile phones to be essential when their children are travelling to and from school.

Devices should not be used in school without the permission or as guided by a member of staff. Devices are used to enhance or transform learning and are not used socially. All devices should be 'out of sight' during the day and turned off or on silent.

Parents of Secondary students receive the following letter at the start of each term:

"The Ministry of Education does not allow students to use mobile phones within the school premises. If, however, you feel that your child needs to have a mobile phone for use to and from school, then your child's phone **will be kept with the Secretary to the Principal or in your locker** until the end of the day. Please bear in mind that phones are NOT allowed during the school day. If your child is found to use the phone at break or in lessons, the item will have to be confiscated. Likewise, if your child has a phone in school without a consent declaration by you, then the phone will have to be confiscated. Parents will be asked to collect the item at the end of the school or for repeat offenders at the end of the week.
The decision to provide a mobile phone to their children should be made by parents or carers.

If you allow your child to bring his/her mobile in school please be aware that:
• Mobile phones should be switched off and kept in the locker. The school cannot accept responsibility for any loss, damage or costs incurred due to its use.
• Students may only use their mobile phones in the classroom when express permission has been given by the teacher. The use of personal mobile phones in one lesson for a specific purpose does not mean blanket usage is then acceptable.
• Mobile phones must not disrupt classroom lessons with ringtones, music or beeping. Using mobile phones to bully and threaten other students is unacceptable. Cyber bullying will not be tolerated.
• It is forbidden for students to "gang up" on another student and use their mobile phones to take videos and pictures of acts to denigrate and humiliate that student and then send the pictures to other students or upload it to a website for public viewing. This also includes using mobile phones to photograph or film any student or member of staff without their consent.
• Mobile phones are not to be used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.
• It is unacceptable to take a picture of a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images.

If you wish to give consent for your child to bring his/her mobile phone into school please click here:

https://bit.ly/kiesphoneconsent
or

https://form.jotform.com/21273273624

Communications

- mobile phones and other devices must be kept in silent mode during the school day;
- students may not use mobile phones to receive or send text messages or phone calls during the school day.
- if parents need to urgently contact their child, or if students need to make a phone call to their parents, they should do so through Reception.

- staff may not use mobile phones during lessons or when on duty. They should take care to be discrete at other times so as not to disturb other members of the school or for others to hear personal information, and should not use mobile phones in the hallways;
- the use of mobile phones and other mobile technologies may be allowed within a learning situation, with the permission of the member of staff who is in charge at that time;

Digital Imaging

- the use of digital equipment to take photos of students, staff or of the school is not allowed except with the express permission of a member of staff. Even when such permission has been given the permission of the individual – or the parent of the individual - concerned must also be gained;
- images of students, staff or of the school may not be posted on public or private web sites, or transferred or given to another person, without the permission of the Principal;
- the use of digital equipment to take photos of in EYFS is not allowed except with the express permission of the Principal or authorized member of staff.

Music Players

- students should not have earphones or similar technology on show, and should remove these when entering the building.

Social Media

Many adults and children regularly use social media to engage and communicate, as does the school, especially when such engagement can be used to enhance learning and teaching. Whilst the use of social media is, therefore, encouraged, it is vital that staff and students use these technologies and services effectively and responsibly. The use of social networking applications, in particular, has implications for the school's duty to safeguard children and young people.

Definitions

Social media applications include, but are not limited to, blogs and microblogging applications, online discussion forums, collaborative spaces, media sharing services and online gaming environments. Examples include Instagram, WhatsApp, Twitter, Facebook, Messenger, YouTube, Flickr, online gaming platforms, etc, and include comment streams on public websites such as newspaper sites. Of particular benefit and use in school, these also include Google Classroom, Class Dojo or virtual homework diaries. As it is impossible to cover all circumstances or emerging media, the principles set out in this Policy must be followed irrespective of the medium, and also apply to other types of online activities.

For the purpose of this Policy, the term '*social media*' also applies to the use of communication technologies such as mobile phones, cameras, iPads, laptops and other computer devices and any other emerging forms of communications technologies.

Principles

All members of the school community need to be aware that everything they post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed and it is easy to lose control of it. They should therefore assume that everything they post online will be permanent and will be shared.

All individuals are responsible for their own actions and conduct, and should avoid behaviour which might be misinterpreted by others or which could put them in a position where there is a conflict between KIES and their personal interests. Staff should also avoid behaviour which could put them in a position where there is a conflict between their work for KIES and their personal

interests. Staff actions should not bring the school into disrepute.

Within this Policy, there is a distinction between the personal use of social media and the school-sanctioned use of social media for professional educational purposes.

Use of Social Media

Social Networking

All e-mail communication between staff and members of the school community on school business must be made from an official school e-mail account.

Staff members must be conscious always of the need to keep personal and professional lives separate and to always maintain appropriate professional boundaries. Staff should not use personal email accounts or personal mobile phones to contact students, nor should any such contact be accepted, except in circumstances given prior approval by the Principal. In the case of school trips, staff should make it clear when completing risk assessments that they will require student contact numbers. Student contact details must be deleted after the trip.

Staff should not use personal email accounts or personal mobile phones to contact students, nor should any such contact be accepted, except in circumstances given prior approval by the Principal. In the case of school trips, staff should make it clear when completing risk assessments that they will require student contact numbers. Student contact details must be deleted after the trip.

Social Networking

The use of social networking applications for personal use during school time is not permitted.

General guidance for members of the KIES community about the personal use of social networking applications is given in *Appendix 1*, below.

Staff members must be conscious at all times of the need to keep personal and professional lives separate and to always maintain appropriate professional boundaries. They may not use school e-mail addresses or other official contact details for setting up personal social media accounts or for communicating through social media, and the school's logos must not be used or published on personal webspace.

Social networking sites have the potential to discuss or publish inappropriate information. Therefore, all members of the KIES community should consider the reputation of the school in any posts or comments relating to the school on social media accounts. Apart from via official school accounts, staff are required to avoid posts or comments that refer to specific matters relating to the school and/or individual members of its community.

Confidentiality must be considered at all times. All members of the KIES community are strongly advised to set privacy settings to the highest possible levels on all personal social media accounts. Staff members must not publish on their personal webspace any confidential information to which they have access as part or as a result of their employment at KIES. This includes personal information about students or their family members, colleagues or other school-related information. This requirement continues after the staff member has left KIES employment.

Staff members must not establish, or seek to establish, social contact via social media or other communication technologies with students. They must never "friend" a student currently attending KIES or an ex-student who is eighteen years old or younger. Staff members should only access students' social networking sites under agreed circumstances with the explicit permission of the Principal.

If any member of the school community is aware of inappropriate communications involving

any student in any social media, these must immediately be reported to the Principal. Inappropriate communications may include:

- personal communications between students and teachers;
- the use of social media to attack, insult, abuse or otherwise make negative, offensive or discriminatory comments about students, their family members, colleagues, the school or other organisations;
- the browsing, downloading, uploading or distribution in school of material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.

School-sanctioned Use of Social Media

KIES provides education in School-sanctioned use of social media in the form of many ways (listed in the Digital Citizenship section).

There are many legitimate uses of social media within the curriculum and to support, enhance and develop students' learning. Staff who use Social Media as part of their curriculum should refer to the following links to support the promotion of e-safety:

- https://www.thinkuknow.co.uk/
- https://www.betterinternetforkids.eu/
- http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx
- http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety- features

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Principal. The use of social networking applications which are not related to any school services (e.g. contributing to a wiki provided by a professional association) does not need to be approved by the Principal, but KIES users must still operate in line with the expectations set out within this Policy (*Appendix 1, below*).

Members of the KIES community must adhere to the Guidelines, which apply to all uses of social networking applications by school representatives (*see Appendix 1, below*). This includes, but is not limited to, the use of public-facing applications (such as open discussion forums) and internally-facing uses (such as project blogs), regardless of whether they are hosted on the school network or not.

If staff set up a social media site or account for educational purposes, it should be entirely separate from any personal social media accounts held by that member of staff, and should be linked to an official school e-mail account. Any site should include a link to the Acceptable Use Policy on the school website and any links to external sites must be regularly checked to ensure they are appropriate and safe. All content should be solely professional and should reflect well on the school. Photographs should not identify by name any student and personally identifying information must not be published

Engagement Approaches

Engagement and education of children and young people

- An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- Education about safe and responsible use will precede internet access.

- Students input will be sought when writing and developing school online safety policies and practices.
- Students will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Student instruction regarding responsible and safe use will precede Internet access. Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study.
- Online safety (e-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments.
- The student Acceptable Use expectations and Posters will be posted in key locations.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety (e-Safety) education approaches.
- The school will reward positive use of technology by students.
- The school will implement peer education to develop online safety as appropriate to the needs of the students.

Engagement and education of children and young people who are considered to be vulnerable

- KIES is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate.

Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
- To protect all staff and students, the school will implement Acceptable Use Policies which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the leadership team and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Engagement and education of parents and carers

- KIES recognises that parents/carers have an essential role to play in enabling children

to become safe and responsible users of the internet and digital technology.

- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement. Parents will be encouraged to read the school Acceptable Use Policy for students and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

Breaches of this Policy

The school addresses any incidents of inappropriate behaviour which involves members of the school community, whether inside and outside of school, through the Positive Behaviour Policy and the Staff Code of Conduct/Behaviour Policy. Failure to comply with this Policy and the Acceptable Use agreement will lead to disciplinary action in accordance with these policies.

The use of IT to harass or bully another individual is a serious breach of the school's ethos and policies. Cyber-bullying, the use of images without permission or misusing the personal information of others will be dealt with most severely.

'Minor' breaches of this Policy by students, such as using mobile technologies at inappropriate times, will result in the confiscation of the device. On the first offence, the item will be returned at 14:00 – at the end of the school day. For subsequent offences, mobile phones will be returned at the end of the week and the parent will be informed. Other technology items will not be returned until the school receives a request letter from the parent/guardian.

For other breaches of the Policy, parents will be notified and students may be denied access to the school network and internet, as well as other sanctions (including exclusion).

Any breach of this Policy by a staff member will lead to disciplinary action, including the possibility of dismissal.

APPENDIX 1: Guidelines for the Use of Social Media

Personal Use of Social Media

All members of the KIES community should:

- use social media in a professional, responsible and respectful way and must comply with the law, including equalities legislation, in on-line communications;
- not represent their personal views as those of the school on any social medium;
- not engage in activities involving social media which might bring the school into disrepute;
- not use social media or the internet in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about students, their family members, staff, the school or other related professionals or organisations.

In addition, KIES staff must:

- be conscious at all times of the need to keep personal and professional lives separate and to always maintain appropriate professional boundaries;
- act in the best interests of children and young people when creating, participating in or contributing content to social media sites;
- not name or otherwise identify students, former students or their parents and family members in social media conversations;
- not discuss personal information about students, their family members, colleagues or any other professionals or organisations they interact with as part of their job on social media;
- not browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.

School-Sanctioned Use of Social Media

When using social media for educational purposes, the following practices must be observed:

- Staff who use Social Media as part of their curriculum should refer to the following links to support the promotion of e-safety:

  https://www.thinkuknow.co.uk/

  https://www.betterinternetforkids.eu/

  http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

- Staff may set up a distinct and dedicated social media site or account for educational purposes with the prior approval of the Principal.

  This must be entirely separate from any personal social media accounts held by that member of staff, and must be linked to an official school e-mail account.

  It should include a link in the About or Info page to the e-Safety & Acceptable Use of IT Policy on the school website. This will indicate that the account is officially sanctioned by the school.

- The content of any school-sanctioned social media site should be solely professional and

should reflect well on the school.

It must adhere to the guidelines for each social networking site:
http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety- features

Care must be taken that any links from the account to external sites are appropriate and safe.

- The school has a list of any students who may not appear in photographs on school media.

  On other school-sanctioned media, staff must not publish photographs of children without the written consent of parents/guardians, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts.

- Staff should not engage with any direct messaging of students through social media where the message is not public.

- Any inappropriate comments on or abuse of school-sanctioned social media should immediately be removed and reported to the Principal.

APPENDIX 2: Acceptable Use Agreement

This agreement should be completed by students and staff after reading the e-Safety and Acceptable Use of IT Policy.

Once you have signed this agreement you will be given an individual school e-mail address and have access to KIES's ICT systems.

User Agreement

I have read the KIES e-Safety and Acceptable Use of IT Policy and agree to abide by its guidelines on all occasions, in particular when:

- I use KIES ICT systems and equipment, both inside and out of school.
- I use my own ICT equipment in school such as mobile phones, tablets, PDAs, cameras, laptop computers.
- I use my own equipment out of school in a way that is related to my being a member of the school, such as communicating with other members of the school and accessing the Internet to complete homework assignment.

Additionally, this following agreement should be completed by parents of KIES students after reading the e-Safety and Acceptable Use of IT Policy:

KIES Parents in Partnership

I have read KIES's e-Safety and Acceptable Use of IT Policy and understand that although the school will do all it can, it cannot ultimately be held responsible for the nature and content of material accessed on the Internet and using mobile technologies.

I will encourage my child to adopt safe use of the internet and other technologies at home and inform the school if I have any concerns regarding my child's e-safety.

I give permission for my son/daughter's photograph to be used on the KIES website and other publications that have been authorised by KIES.

Review and Evaluation

This policy is to be reviewed and evaluated every two years by the SLT and Principal.