E-Safety Policy 2017

This policy was reviewed and ratified by the Guidance Committee on 24/5/2017.

Background to the Policy

- Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Communication Policy

An e–Safety training programme raises the awareness and importance of safe and responsible internet use.

- Student instruction in responsible and safe use should precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and ICT programmes covering both safe school and home use.
- e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and through assemblies. Particular attention will be given where students are considered to be vulnerable.

How will the E-Safety Policy be Discussed with Staff?

The e–Safety Policy will be formally provided to and discussed with all members of staff.
To protect all staff and students, the school will implement Acceptable Use Policies.
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 the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

Introduction of the Policy to Staff, Students and Parents

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource. All students must apply for Internet access individually by agreeing to comply with the e–Safety Rules. Parents will be asked to sign and return a consent form for student access.

Importance of Internet Use

Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

Benefits of Internet use to Education

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with KCC and DfE;
- Access to learning wherever and whenever convenient.

Enhancing Learning

The school's Internet access will be designed to enhance and extend education.

Learning Platforms

Students/staff will be advised on acceptable conduct and use when using the learning platform. Only current students, parents/carers and current members of staff will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be

carried out before use in school is allowed. It is recognised that smart phone technologies and other similar devices are able to present a degree of risk where students use independently purchased data contracts from mobile phone providers. It is parents' responsibility to ensure that their child's mobile device's access is filtered to prevent access to such inappropriate material.

The school recognises the usefulness of smart phones for students both as a way of contacting parents and as a medium for learning. However, students may use mobile technology to assist them with learning within lessons only when given approval by teacher. Within tests and examinations mobile phones are prohibited.

Teaching Students to Evaluate Internet Content

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The school will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.

- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Security of School Information Systems

The security of the school information systems and users will be reviewed regularly.
Virus protection will be updated regularly.

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission followed by a virus check.
- Unapproved software will not be allowed in students' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.

Assessment of Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.

Social Media and Social Networking Sites

The school will control access to social media and social networking sites though appropriate filters on the school network. Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- Staff members should not have current students as friends on social media sites like Facebook, Instagram, Snapchat etc or engage in conversations of a personal nature with students over the Internet. However it is recognised that staff may wish to join friendship groups of other colleagues on these types of site. Teachers may also use these sites for setting up groups for posting homework etc.
- If personal publishing is to be used with students then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Students should be advised on security and encouraged to set passwords and deny access to unknown individuals. They should be instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. The school behaviour policy will be used in cases where such instances have occurred.
- If staff or students discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.

School Website

The contact details on the website should be the school address, email and telephone number. Staff or students' personal information must not be published.

- The Headteacher and Head of School will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Images that include students will be selected carefully for the school website and intranet site.

Student E-mail

Students must immediately tell a member of staff if they receive offensive email. Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

Cyberbullying and Other Anti-Social or Offensive Activities

Cyberbullying (along with all forms anti-social or offensive activities) will not be tolerated in school. This includes students making offensive remarks about teachers or other students in the school. There will be clear procedures in place to support anyone affected by these forms of behaviour.

- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:
    - Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
    - The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

E-Safety Complaints

Complaints of Internet misuse will be dealt with under the School's Complaints Procedure. Any complaint about staff misuse must be referred to the headteacher. All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

- Students and parents will be informed of the complaints procedure.
- Parents and students will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.