E-Safety Policy

Aims

- To safeguard the welfare of students and staff
- To ensure security and confidentiality
- To safeguard the facilities and support student behaviour
- To provide students with a safe high quality ICT experience as an essential part of their learning

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.

General Statement

The School 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 and the 'Every Child Matters' agenda, 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 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.

E-mail

Students do not have access to a school email account, however in certain circumstances there may be occasions where student to teacher or teacher to student communication may occur.

- 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 Head 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.
- Students' full names will be avoided on the Web site, particularly in association with photographs.
- Permission from parents will be obtained before photographs of students are published on the school website.

Social networking

- 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 Data 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.
- Staff will use a school phone where contact with students is required.

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' 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.
- 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.

- 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 Head of Data & Attainment.
- Any complaint about staff misuse must be referred to the Head.
- 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' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents may 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 enter their child to 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 Head of Data & Attainment, who will then communicate issues of concern to the Head of Education 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 Data Manager.
- Teaching staff are required to deliver E-safety lessons to classes.
- 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 or tutor 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 Data Manager considers it appropriate with a student at possible serious risk, the Head of Education will be asked to intervene with appropriate additional support from external agencies.

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.

Senior students (age appropriate) will also be made aware of the dangers of adult entertainment and violence on the internet; as well as the danger of extremist views.

Staff

All staff are responsible for using the school ICT systems and mobile devices in accordance with the school Acceptable Use Policy (AUP) 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 parents and students must be professional in tone and content at all times. 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 Data Manager and subject leader without delay.

Behaviour

The School 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 cyber bullying.

Sanctions

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 or Head of Education;
- Informing parents;
- Removal of Internet or computer access for a period
- Internal and external exclusion

Any complaint about staff misuse will be referred to the Head of Education and may result in formal disciplinary proceedings. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy with possible police involvement. Complaints related to child protection are dealt with in accordance with school Safeguarding Policy.

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 senior leadership team, 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.