ROSE BRIDGE ACADEMY

E-Safety Policy

Revised Date: October 2016

Aim

The E-Safety policy and procedures are to ensure young people use new technologies in a way which will keep them safe, without limiting their opportunities for creation and innovation.

Purpose

The Internet and digital communications are an essential toolset in the 21st century for education, business and social interaction. The school computer system and Internet access is designed expressly for student use and will include filtering appropriate to the age of the students. Clear boundaries will be set for the appropriate use of the computer system, the Internet and digital communications for staff and students.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies

Additional Relevant Policies

- Student ICT Acceptable Usage Policy
- Staff ICT Acceptable Usage Policy
- Safeguarding Policy
- Bullying Policy

Requirements

All staff, students and parents/guardians of students must read and sign that they have read and agree with:

- ICT Acceptable Usage Policy

Staff Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Responsibility	Role	Staff member responsible
E-Safety Coordinator / Officer	Deputy Headteacher	V Schumacker
E-Safety Monitoring	Deputy Headteacher / Pastoral Team	S Blade, P Burrows, N Smith, K Seeds, J Raughter, S Heaton
Student Guidance on ICT Use	Subject Leader: Computing	I Flynn
Security of ICT Systems	ICT Manager	L Owen
Ensuring E-safety when using technologies	All Staff	All Staff
Approval of Policy	Governing Body	Governing Body

E-Safety Coordinator / Officer
Responsible for:

- Ensures day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with pastoral team to discuss current issues, review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team

E-Safety Monitoring
Responsible for:

- Following the procedures for system checks as listed
- Keeping accurate records of monitoring software outputs
- Weekly report to person responsible for E-Safety Officer
- Any issues identified are reported to the person responsible for E-Safety and to the designated person on the pastoral team and the member of SLT responsible for Safeguarding.
- Following all policies related to E-Safety
- Reporting serious issues to the relevant authority / E-Safety Office.

Student Guidance on ICT Use
Responsible for:

- Planning and delivery of lessons by the ICT department on E-Safety
- Reporting serious issues to the relevant authority / E-Safety Officer
- Assemblies on bullying(cyber-bullying) / Safer Internet
- Reporting serious issues to the relevant authority

Security of ICT Systems
Responsible for:

- Ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the school meets the e-safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- Make certain that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Ensuring the school's filtering policy is applied and updated on a regular basis
- Ensuring that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /

Headteacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction

- Implementing system monitoring software and ensuring they are up to date.

All Staff
are responsible for ensuring that:

- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co Officer / Headteacher / Senior Leader / Class teacher / Head of Year for investigation / action / sanction
- digital communications with students / pupils (email) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended school activities using system Monitoring software
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Governing Body
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Students

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. This is currently done electronically using system monitoring software.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies; Including the use of mobile phones. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

System Monitoring / Filtering Software

Rose Bridge Academy have chosen Impero Education Pro as their E-Safety system monitoring solution. Impero E-Safety Features:

- prevent access to unsuitable sites
- prevent unauthorised use of proxy sites
- enforce acceptable usage policy
- create key word libraries for real-time detection
- monitor using specialist built-in key word libraries
- determine potential risk through key word glossaries with explanations
- create different policies depending on severity
- capture time stamped screen shots of every violation
- add screenshots to logviewer report
- record on-screen activity and specify recording length to capture misuse
- export violations with details and image to PDF
- evidence misconduct from a centralised log to support disciplinary action
- alert the relevant authority when rules are violated
- apply policies and filters to laptops when disconnected from the network
- log and monitor all web activity
- enable students to anonymously report concerns using the Confide system
- real-time monitoring of mobile devices including iPads and Chromebooks

Web filtering, firewall rules and application control is managed and enforced by Sophos.

Education

Students

Whilst policies and technical solutions have been implemented to protect students, it is also important to educate them to take a more responsible approach. The education of students in e-safety has therefore become an essential part of the Academy E-Safety provision.
Rose Bridge Academy provide e-safety provision in the following ways:

- An e-safety programme is provided as part of Statutory ICT / PHSE / other lessons and is regularly revised.
- Key e-safety messages are reinforced as part of a planned programme of assemblies.
- Students are reminded in all lessons to be critically aware of the materials / content they access on-line and are directed to safe content using content whitelists where necessary.
- Students are encouraged to read and understand the Academy ICT AUP and to adopt safe and responsible use of ICT, the internet and mobile devices both in school and at home.
- Students are presented with the Academy AUP on first login and when any amendments are made to which they must agree to in order to proceed with login.
- Educational material to be on display in classrooms / offices as a reminder to the risks that surround the use of technologies.

Parents

Many parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children in the monitoring / regulation of the children's on-line experiences. This is often referred to as the generational digital divide. Parents often underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The Academy will provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents / information evenings

It is also assumed that parents will act as good role models and promote good and safe use of ICT.

Staff

It is essential that all staff receive relevant e-safety training and have a good understanding of their role and responsibilities.

- A planned agenda of e-safety training will be made available to staff.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy e-safety policy and Acceptable Use Policies.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals and groups as required.
- Staff are encouraged to read and understand the Academy ICT AUP and to adopt safe and responsible use of ICT, the internet and mobile devices both in school and at home.
- Staff are presented with the Academy AUP on first login and when any amendments are made to which they must agree to in order to proceed with login.
- The ICT Manager will circulate tips on how to stay safe in addition to updating staff with current news, trends and threats.