October 2021

Rugby High School

E-Safety Policy

Rugby High School believes that the use of information and communication technology in school brings great benefits. This policy aims to recognise e-safety issues and will help to ensure the appropriate, effective and safer use of electronic communications for all pupils and staff.

We are aware that in today's society children, young people and adults interact with technologies such as; mobile devices (including phones, tablets, wearable technology e.g. smart watches), games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. E-Safety encompasses the safe use of all electronic devices and their associated software which can be used to send, store or create messages, data and documents. These include internet technologies and electronic means of communication such as mobile phones and wireless technology.

The Academy acknowledges that it has a key role to play in educating children and young people and the parents and carers about the benefits and risks of using new technology. It has a responsibility to provide safeguards for users while developing students' awareness so that they can enjoy online experiences in safety.

The Academy's e-safety policy operates in conjunction with other policies including those for Student Behaviour, Bullying, Child Protection, Curriculum, Data Protection and Security.

Scope

This e-safety policy covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communication technologies, both in and out of school.

Aims

1. To safeguard children, young people and employees.

2. To be able to identify the risks associated with social networking.

3. To identify roles and responsibilities and recognise that e-safety is part of the 'duty of care' which applies to everyone working with children.

4. To educate and empower children so that they possess the necessary skills to make safe and responsible decisions and to feel confident to report any concerns they may have.

5. To raise awareness of the importance of e-safety amongst all employees so they are able to educate and protect children in their care.

6. To inform employees how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

7. To provide opportunities for parents/carers to develop their knowledge of e-safety.

8. To ensure awareness amongst all members of Rugby High School that ‘online actions can have offline consequences’.

Forensic Monitoring and Filtering

All school owned or leased equipment has forensic monitoring software installed on it which is used to monitor usage 24/7. In addition, the Academy uses a filter to screen out inappropriate or unsuitable content.

The Academy 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 Academy cannot accept liability for the material accessed, or any consequences of Internet access if the students do not follow the rules in the acceptable user policy.

Student Wifi

Students will access the BYOD WIFI system through their school network username and password. The WIFI is free for students and will allow filtered access to the internet as controlled by the Academy. It is strongly recommended the students use the RHS Public network whilst on school premises to stay safe online. The Academy cannot be responsible for the material accessed by a student if they connect to the internet through their own data connection.

E-Safety Coordinator

The Academy’s E-Safety Coordinator is the Designated Child Protection Teacher/Officer as the roles overlap. This person has responsibility for ensuring that staff receive regular training in regard to e-safety; that policies (including the ICT User Agreements) are kept up to date; signed and followed; that students receive appropriate training on e-safety matters as part of their PHSE and ICT lessons and that they are able to put the training that they receive into practice.

Reporting Incidents and Complaints

An E-Safety incident is any incident which involves the use of electronic technology e.g. email, mobile phone texts, digital images/videos etc. All incidents relating to e-safety should be reported to the E-Safety Co-ordinator.

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

If staff or students discover unsuitable sites, the URL (address), time, content must be reported to eSafe via the E-Safety coordinator. In cases where there is a potential child protection issue the person reporting the matter should speak directly to the Designated Person and follow up the conversation with a My Concern incident form. Where applicable, referrals may be made to the MASH (under the Child Protection Procedures) and/or CEOP (The Child Exploitation and Online Protection Unit).

Internet Usage, Access and Monitoring

Internet usage is an essential part of a twenty-first century education. Access to the internet can provide students with many educational benefits and can help them to develop their capacity to learn independently. Students will be taught what Internet use is acceptable and what is not. Students will be reminded at regular intervals about how to keep themselves safe on line and what to do if they feel that their safety is compromised in any way or if they are being bullied or harassed.

They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Staff will guide students in on-line activities.

Whilst students are in school, the Academy can monitor and filter their internet access, however, students use the Internet outside school and therefore need to learn how to evaluate internet information and to take care of their own safety and security.

Students are given access to the internet in school on condition that they abide by the terms of the school's Student ICT User Agreement. Students who misuse ICT equipment, who break the terms of the User Agreement or who use their access to bully or harass others will have their accounts frozen for a fixed period and run the risk, if the behaviour is repeated, of permanently losing their access. Where appropriate, the Academy will report instances of abuse to external agencies (including the police).

All staff must read and sign the 'Staff ICT User Agreement' before using any school ICT resource. Parents/carers and students will be asked to sign and return the ICT User Agreement before a student can use the school's ICT equipment.

Email

Students may only use approved school e-mail accounts on the school system and should use these accounts whenever communicating with teachers. Students should 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 others (the exception to this is where the arrangement to meet relates to an official school activity).

Social Networking

Students are advised never to give out personal details of any kind which may identify them or their location. They are advised not to place personal photos on any social network space and are encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. They are encouraged to invite known friends only and deny access to others.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.

Responsible use

- Students will be educated on the responsible use of the internet during ICT, PSHE, Form time and assemblies. Students will only use appropriate websites when using the internet at Rugby High School.
- Students should only register with sites where they meet the age requirement this includes social media where you must be 13 Years of age.
- We recommend that passwords are set by parents and monitored for students.
- Students and staff must speak to people respectfully over the internet.
- Students and staff must be aware that their digital footprint stays with them for life.
- Students must not speak to strangers or give out personal details.
- Students and staff must not post inappropriate videos or images.
- Students and staff must gain permission to take videos and images of other students and staff members, as well as check to see if the parent has given written consent to the school for the use of the student in photographs and videos and to make these available for public viewing.
- Students and staff must make no libellous comments about the Academy or staff and students on any internet webpage or media platform.
- Students must immediately report to a member of staff if they or another student receives offensive or abusive emails, text messages or posts on social networking sites.
- Staff must immediately report to the Headteacher if they or any other staff member receives offensive or abusive emails, text messages or posts on social networking sites.

Mobile Phones

Mobile phones can be used on school site by following the School's mobile phone policy.

Mobile phones may be used during lessons with the teacher's permission to photograph work, record or to conduct research. The sending of abusive or inappropriate text messages and the taking of images of individuals without their consent is forbidden.

Staff should not use their own phones to contact students. They will be issued with a school phone where contact with students is required.

BYOD

Students are permitted to bring in their own device into school, this includes laptop, tablet and mobile phone. The device is used at the risk of the student and the Academy accepts no responsibility to damage or loss of the device.

Any device supplied by the Academy will have forensic monitoring software installed and will be monitored following the School's BYOD policy.

Published Content and the School Web Site

Staff or students' personal information will not be published on the Academy's website and care will be taken to ensure that students' anonymity is protected.
The headteacher has overall editorial responsibility for the website and for ensuring that content is accurate and appropriate.

Publishing Students' Images and Work

Photographs that include students will be selected carefully and students' names will not be used in association with photographs. Written permission from parents or carers will be obtained before photographs of students are published on the Academy's website or used for other purposes. Students' work will only be published with the permission of the student.

Information System Security

The Academy's ICT systems capacity and security will be reviewed regularly. Virus protection is installed and is updated regularly.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Academy's Data Protection and Freedom of Information Policy and the GDPR Policy. All students and their parents will be asked to sign a Fair Processing Notice.

Safeguarding – please refer to the Safeguarding policy.

Bullying – please refer to the Bullying policy.

Prevent and Peer on peer – please refer to the Child Protection Policy.

Child Protection – please refer to the Child Protection Policy.

Communication of Policy

Students

- Students will be informed that Internet use will be monitored
- If students search for inappropriate websites, they will be spoken to by a senior member staff at the Academy.
- If students type inappropriate comments they will be spoken to by a senior member staff at the Academy.

Staff

- All staff will be given the Academy's E-Safety Policy and 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.
- Staff will be given clear training on the Academy's E-safety policy and how to use the school IT equipment.
- Further employee guidance for personal use and social networking will be discussed as part of the employee induction process (including NQT and SCITT programmes)

and safe and acceptable professional behaviour will be outlined in the Employee Acceptable Use Policy

- Staff will be directed to and expected to complete Esafety training every academic year

Parents

- Parents' attention will be drawn to the Academy's E-Safety Policy in newsletters, the school prospectus and on the school website.

The E-Safety Policy will be reviewed annually.

October 2021

Referral Process – Appendix A

E-Safety Rules– Appendix B

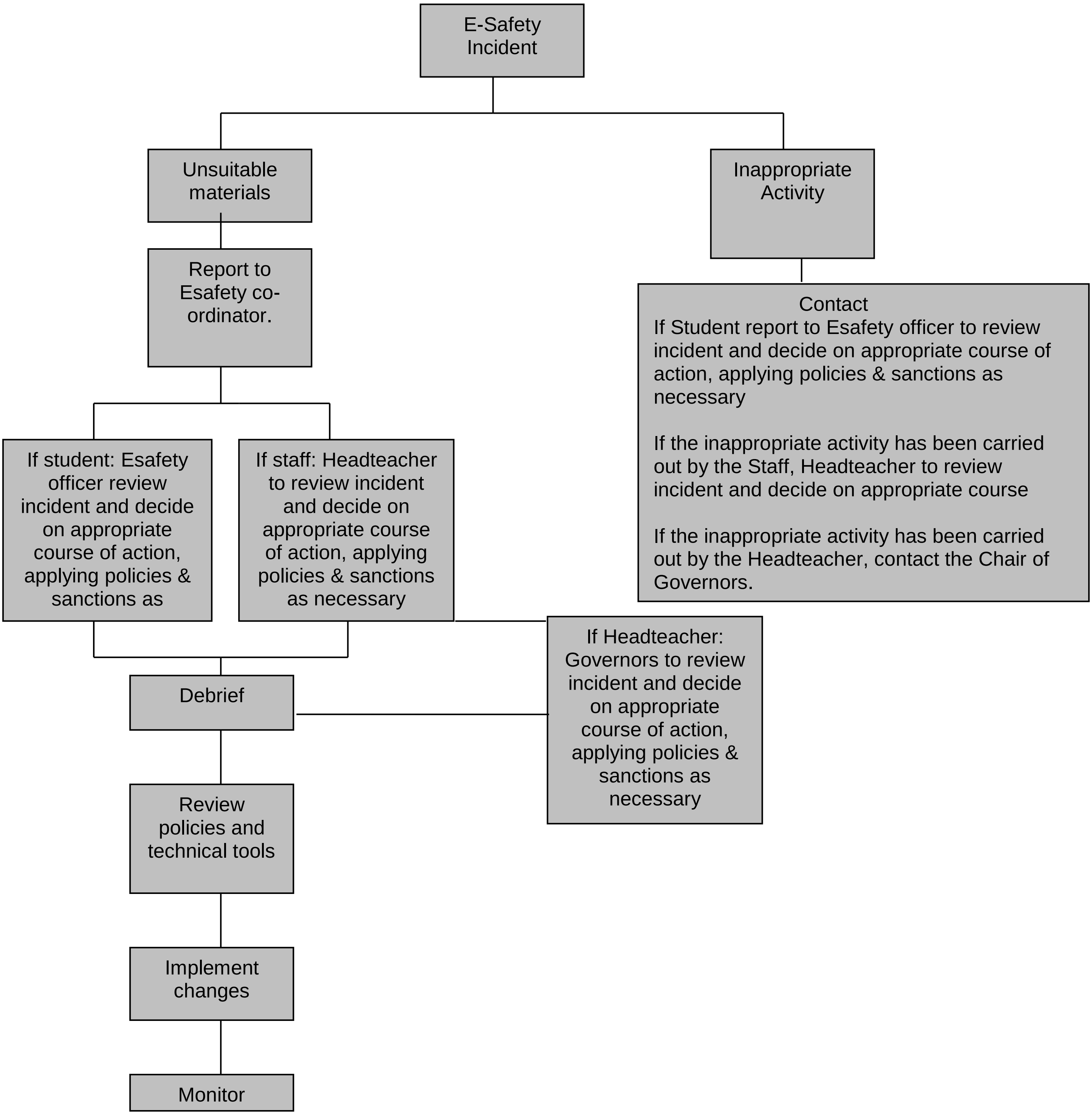
Student ICT User Agreement– Appendix C

Staff ICT User Agreement – Appendix D

Useful Sources of Information, Advice and Support re E-Safety – Appendix E

Appendix A

Flowchart for responding to e-safety incidents in school



E-Safety Incident

Unsuitable materials

Report to Esafety co-ordinator.

If student: Esafety officer review incident and decide on appropriate course of action, applying policies & sanctions as

If staff: Headteacher to review incident and decide on appropriate course of action, applying policies & sanctions as necessary

Debrief

Review policies and technical tools

Implement changes

Monitor

Inappropriate Activity

Contact

If Student report to Esafety officer to review incident and decide on appropriate course of action, applying policies & sanctions as necessary

If the inappropriate activity has been carried out by the Staff, Headteacher to review incident and decide on appropriate course

If the inappropriate activity has been carried out by the Headteacher, contact the Chair of Governors.

If Headteacher: Governors to review incident and decide on appropriate course of action, applying policies & sanctions as necessary

Adapted from Becta – E-Safety 2005

Appendix B

E-Safety Rules

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

- The Academy owns the computer network and can set rules for its use. The school network (and internet access) is only to be used for educational purposes. Use for private purposes, personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted. N.B. It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use of the Academy's ICT equipment may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password. You must not give your password to any other person or allow them to use your account.
- Copyright and other intellectual property rights must be respected.
- Access to some social networking sites, chatrooms and instant messaging services is currently not allowed in school.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers. Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- Students may not install programmes on school ICT equipment except when working under the supervision of an ICT teacher and with the permission of the school's network manager.
- You may not bring food or drink into an ICT room.

The Academy operates a filtering system which means that access to some sites is denied. In addition, it uses software to monitor the use of the Academy's computer systems, including access to web-sites. It may intercept e-mail, delete inappropriate materials and report abuses to external agencies including the police where it believes unauthorised use of the Academy'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.

Appendix C

Rugby High School

Student ICT User Agreement

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 to show that the E-Safety Rules have been understood and agreed.

Student: ***Form:***

Student's Agreement

- I have read and I understand the Academy's E-Safety Rules.
- I will use the computer, network, mobile phones, Internet access, my own device and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: **Date:**

Parent's Consent for Web Publication of Work and Photographs

I agree that my daughter's work may be electronically published. I also agree that appropriate images and video that include my daughter may be published subject to the Academy's rule that photographs will not be accompanied by student names.

Parent's Consent for Internet Access

I have read and understood the Academy's E-Safety rules and give permission for my daughter to access the Internet. I understand that the Academy will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the Academy cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ***Date:***

Please print name:

Please complete, sign and return to the school

Appendix D

Staff ICT User Agreement

- To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this agreement. Staff should consult the Academy's E-Safety policy for further information and clarification. The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand that Academy equipment is provided for use in association with my employment. I understand that use for personal financial gain, gambling, political activity or illegal purposes is not permitted.
- I understand that usage of all school equipment is monitored, monitoring is comprehensive and occurs whenever and wherever equipment is used, 24 hours of the day, 365 days of the year
- I understand that I am required to maintain the Academy's reputation and standing in the community and not to do anything which would damage public trust or confidence in the teaching profession. I understand that I must maintain professional standards at all times including using language appropriate to my professional status.
- I understand that staff using school equipment to access pornography or adult only sites and materials; to send or post messages of an intimate or suggestive nature will be subject to disciplinary proceedings and may face dismissal for gross misconduct.
- I understand that staff who breach the staff behaviour policy though school equipment will be held accountable through the Academy's staff behaviour policy.
- I understand that school information systems may not be used for private purposes or for advertising, without specific permission from the headteacher.
- I understand that the Academy may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school E-Safety Coordinator or the Designated Safeguarding Lead.
- I will ensure that any electronic communications with students are compatible with my professional role. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority. I will not create or send messages that could be interpreted as libelous.
- I will use my school email account when communicating with students by email.
- I will not give personal details, including my personal mobile phone number to students and I will not store students' personal details including their mobile phone numbers on my personal phone.

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- The device is to be used for work reasons only.
- The Academy operates a filtering system which means that access to some sites is denied. In addition, it uses software to monitor the use of the school's computer systems, including access to web-sites. It may intercept e-mail, delete inappropriate materials and report abuses to external agencies including the police 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 have read, understood and agree with the Staff ICT User Agreement

Signed: …………………………Capitals: ……………………… Date: ………

Accepted for school: …………………………Capitals: ………………………….