E-Safety Policy

Date: October 2015
Date of review: October 2016

E-Safety
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 provision acknowledges that it has a key role to play in educating students and the parents/carers about the benefits and risks of using modern technology. It has a responsibility to provide safeguards for users while developing students' awareness so that they can enjoy online experiences in safety.

The provision's e-safety policy operates in conjunction with other policies including those for student behaviour, bullying, child protection and curriculum.

Safety Coordinator
The provision E-Safety Coordinator is the Lead Designated Safeguarding Officer, as the roles overlap. This person has responsibility for ensuring that staff receives regular training in regard to e-safety; policies (including the ICT User Agreements) are kept up to date; signed and followed; 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
E-Safety incidents are any incident which involves the use of electronic technology e.g. emails, mobile phone texts, digital images/videos etc. All incidents relating to e-safety should be reported to the E-Safety coordinator, who will log them and review the provision's systems and procedures in the light of them.

Complaints
Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the head teacher. Complaints of a child protection nature will be dealt with in accordance with the p r o v i s i o n child protection procedures.

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the provision's filtering service via the E-Safety coordinator.
- The email address: esafety@queensgatecollege.co.uk should be used both by staff and students wishing to report e-safety issues including instances of cyber bullying.
- In cases where there is a potential Child Protection issues, the person reporting the matter should speak directly to the Designated Safeguarding Officer and follow up the conversation with an email. Where applicable, referrals may be made to Social Care (under the Child Protection Procedures).

E-Safety Policy

Assessing Risks
The provision 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 provision computer. The provision cannot accept liability for the material accessed, or any consequences of Internet access.

The provision will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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 provision, the provision can monitor and filter their internet access; however, students use the Internet outside provision 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 provision on condition that they abide by the terms of the provision'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 access frozen for a fixed period and run the risk, if the behaviour is repeated, of permanently losing their access. Where appropriate, the provision will report instances of abuse to external agencies (including the police).

The provision will maintain a current record of all staff and students who are granted Internet access. All staff must read and sign the 'Staff ICT User Agreement' before using any provision ICT resource. Parent/carer and students will be asked to sign and return the ICT User Agreement before a student can use the provision's ICT equipment.

Email
Students may only use approved provision e-mail accounts on the provision 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 provision activity).

E-Safety Policy

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.

Filtering

The provision subscribes to a filtering service which ensures that its filtering systems are as effective as possible.

Managing Emerging Technologies

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

Mobile Phones

Mobile phones will not be used for personal use during lessons or formal provision time. The only exception to this is when a teacher gives permission for work to be photographed or recorded to aid students' evaluation of it. The sending of abusive or inappropriate text messages and the taking of images in individuals without their consent is forbidden.

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

Published Content and the Provision Web Site

Staff or students' personal information will not be published on the provision's website and care will be taken to ensure that students' anonymity is protected. The head teacher 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 parent/carer will be obtained before photographs of students are published on the provision website or used for other purposes. Students' work will only be published with the permission of the student and her parents.

Information System Security

Provision 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 Data Protection Act 1998. All students and their parents will be asked to sign a Fair Processing Notice.

E-Safety Policy

Communication of Policy

Students

- Rules for Internet access will be posted in all networked rooms
- Students will be informed that Internet use will be monitored

Staff

- All staff will be given the Provision 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.

Parents

- Parents' attention will be drawn to the Provision E-Safety Policy in welcome pack and on the provision website.

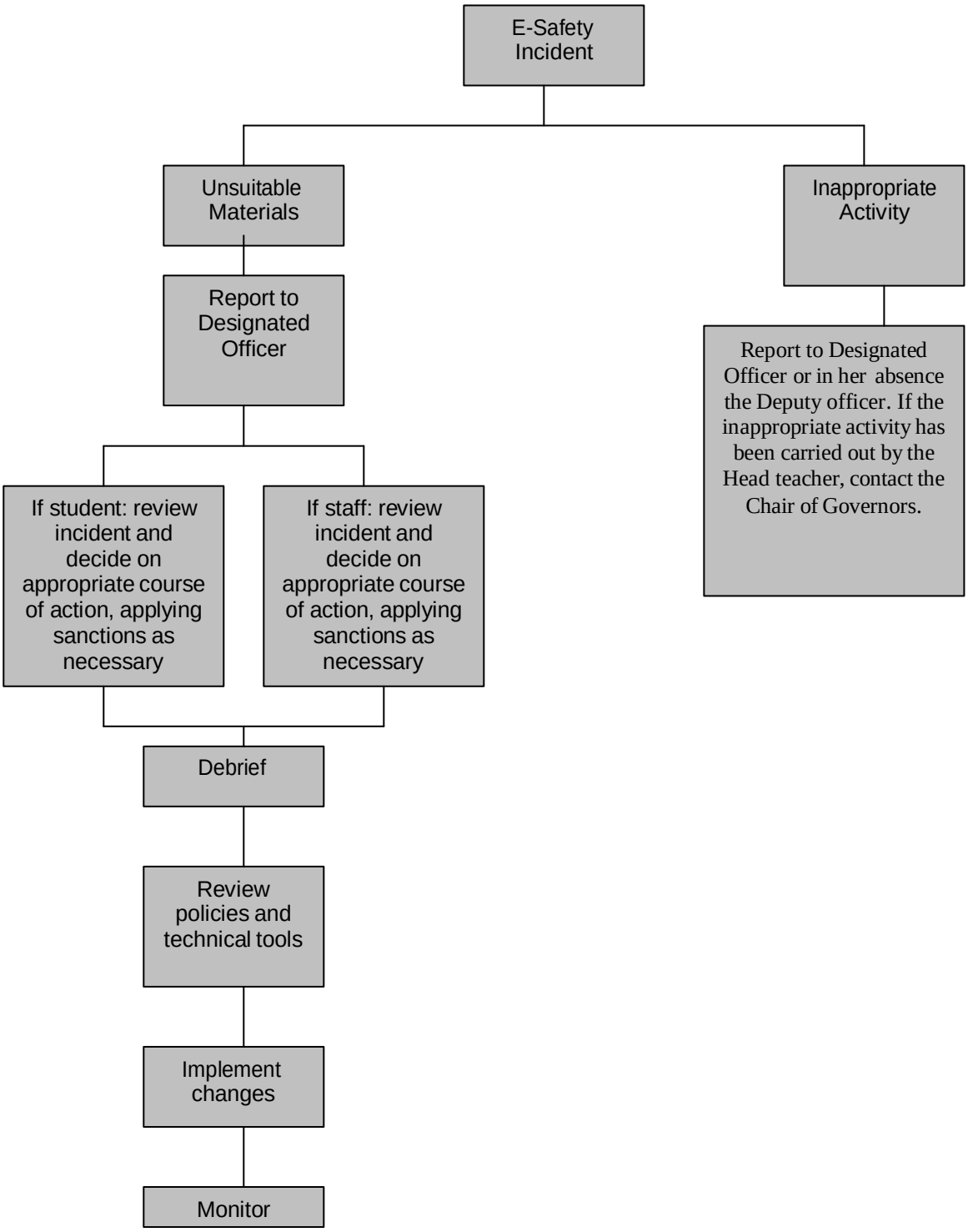
This policy will be reviewed and updated, where necessary, annually

Referral Process – Appendix A

E-Safety Rules– Appendix B

E-Safety Policy

Flowchart for responding to e-safety incidents in provision – Appendix A



E-Safety Policy

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

1. Queensgate College owns the computers, network and can set rules for use. The internet access is only to be used for educational purposes.

    - Use for private purposes, personal financial gain, gambling, political activity, advertising or illegal purposes are not permitted. N.B. It is a criminal offence to use a computer or network for a purpose not permitted by the provision.

2. Irresponsible use of ICT equipment may result in the loss of use and/or Internet access.

3. 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.

4. Copyright and other intellectual property rights must be respected.

5. Access to social networking sites, chat rooms and instant messaging services are not allowed in provision.

6. Messages shall be written carefully and politely, particularly as emails could be forwarded to unintended readers. Anonymous messages and chain letters are not permitted.

7. Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.

8. Students may not install programmes on provision ICT equipment except when working under the supervision of an ICT teacher and with the permission of the Head of Provision.

9. You may not bring food or drink into an ICT room.

The provision operates a filtering system which means that access to some sites is denied. In addition it uses software to monitor the use of the provision'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 provision's computer system may be taking place, or the system maybe being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Queensgate College

E-Safety Policy