Colyton Grammar School
ONLINE SAFETY POLICY

Rationale

The Online Safety Policy relates to other policies including those for ICT, the Acceptable Use Policy (AUP), bullying and for child protection.

The policy is intended to build on current Online Safety Policy guidelines and government guidance.

Teaching and Learning

Why the Internet and digital communications are important

- The Internet is an essential element of 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality internet access as part of their learning experience in school and to teach them to make safe and effective use of the Internet beyond school.
- Internet use is a part of the statutory curriculum and a vital source of learning for staff and students.

Internet use will enhance and extend learning

- School Internet access is designed expressly for staff and pupil use and includes filtering appropriate to the age of students.
- Clear boundaries are set for the appropriate use of the Internet and digital communications and these are regularly discussed with staff and students.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- Students will be helped to understand that the use of Internet derived materials must comply with copyright law. Students are taught to be critically aware of the materials they read. They are shown how to validate information before accepting its accuracy. Students are taught about CSE and prevent in ICT and PSHE lessons.

Managing Internet access information system security

- School ICT system security is reviewed regularly by the Network Manager.
- Virus protection is installed and updated regularly.
- Security strategies will be reviewed at least annually by the Head of Computing and IT, Network Manager, Senior Leadership Team and the Colyton Online Safety Group.

E-mail

- Students may only use approved e-mail accounts on the school system.
- Students are taught:
  - immediately to tell a teacher if they receive offensive e-mails.
  - Not to reveal their personal details or those of others to treat incoming e-mail as suspicious and that attachments must not be opened unless the author is known.
  - not to forward chain emails.

Published content and the school web site

- Staff or student personal contact information is not published. Any contact details given online will normally be those of the school office.
- The head teacher or nominee has nominated the Library and Information Systems Manager to take overall editorial responsibility to ensure that published content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully using only l students whose parental consent has been obtained.
- Students' full names are not used anywhere on the school website, particularly in association with photographs, unless with parental consent. They may be used in newspaper articles as newspapers will not publish without a full name.
- Written permission from parents or carers is obtained when students join the school to allow photographs of students to be published on the school website or in any other medium.
- Work is only published with the permission of the student and parents/carers.
- The consent list is displayed in staff house and is updated by IT support on a yearly basis with the new intake.

Social networking and personal publishing

- The school controls access to social networking sites, and educates students in their safe use. They will be blocked unless a specific use is approved
- Students are given online safety guidance on safe Internet use both in and out of school. This will include the following advice:
    - never to disclose personal details of any kind which may identify them, their friends or their location.
    - never to place personal photos on any social network space without considering how the photo could be used now or in the future.
    - only to invite known friends and deny access to others when using social networking and instant messaging services.
- Students are advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.

Managing filtering

- The school works in partnership with SWGfL to ensure that systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site is being accessed, it must be reported to the Network Manager.
- The Network Manager and Head of Computing and IT are responsible for ensuring that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video-conferencing

- In school videoconferencing over IP will normally use the educational broadband network to ensure quality of service and security rather than the internet.
- Students must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised taking into account the students' age.

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.
- Technologies such as mobile phones with wireless internet access may bypass school filtering systems and present a new route to undesirable material and communications. The Network Manager does all that is reasonably practical to prevent this.
- Mobile phones must not be used during lessons or formal school time for calls or messaging. The sending of abusive or inappropriate text messages is forbidden and will be dealt with in line with the school's anti-bullying policy and AUP.
- The use by students in Y7-10 of smartphones, tablets and cameras in mobile phones will be permitted where there is an identifiable educational benefit but only under staff supervision.

- Students in the Sixth Form, on signing of an acceptable use statement, may access a secure guest Wi-Fi network using a registered device, to support their study in school.
- Games machines including the Sony Playstation, Microsoft Xbox and others have internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location. They may only be used in school with staff permission and supervision.

Protecting personal data

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

Policy Decisions Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy 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.
- Students must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy.
- Parents/carers will be asked to sign and return a consent form based on the appropriate part of the Acceptable Use Policy
- The school will take all reasonable precautions to prevent access to inappropriate material. Due, however, to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access, although it will do all that is possible to reduce the risk of inappropriate material being accessed.
- The Network Manager will monitor the network regularly to establish that the online safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be referred to a member of the Senior Leadership Team.
- Any complaint about staff misuse will be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.

Communicating Online Safety

Introducing the Online Safety policy to students

- The AUP is posted in all rooms where computers are used.
- Students are informed that network and Internet use will be monitored.
- A programme of training in online safety is in place in PSHE and ICT making use of appropriate materials e.g. those from CEOP. This will include online safety issues with students in the autumn term of Year 7.
- We measure impact through assessments in PSHE and Computing. We consider the effectiveness of the strategy overall in departmental reviews in PSHE and Computing.

Staff and the Online-Safety policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff will be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by SLT and work to clear procedures for reporting issues.
- Staff are informed that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to

maintain a professional relationship. They must never use an email account other than their @colytongrammar.devon.sch.uk address to contact students.
- Guidelines for the use of social media sites for educational purposes have been issued to staff along with those for 'safe working practices'
- The Senior Designated Officer (Safeguarding) will assess the impact of training.

Enlisting parents' and carers' support
- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website. The school will maintain a list of online safety resources for parents/carers (see website).

Sanctions
- Minor misuse of school equipment, tablets and mobile phones (such as accessing of games or social media) may result in suspension of online access
- Major misuse of school equipment, tablets and mobile phones (such as accessing age restricted sites, online bullying, tampering with school equipment, hacking school computers and equipment, taking photographs on personal equipment without permission) will be dealt with at the head teacher's discretion.

Equality Impact Assessment
No equality issues have been identified in relation to this policy. Where a behaviour incident may raise an equality issue (e.g. online bullying) this will be dealt with appropriately as identified in the Behaviour Policy.

Consultation
This policy has been consulted upon with the Designated Senior Person (Safeguarding), the Head of Computing and IT, the Network Manager and the Colyton Online Safety Group.