The Cavendish High Academy e-safety policy

Teaching and learning

Why the Internet and digital communications are important

- 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 high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning

- The Cavendish High Academy Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The Cavendish High Academy will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- The Cavendish High Academy's ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail
- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The Cavendish High School Academy 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

- Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
- The headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing students' images and work
- Photographs that include students will be selected carefully so that individual pupils cannot be identified or their image misused.
- Students' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Work can only be published with the permission of the student and parents/carers.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate students in their safe use.
- 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, their friends or their location.
- Students should not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block

unwanted communications. Students should only invite known friends and deny access to others.

Managing Filtering

- The Cavendish High Academy will work in partnership with Becta, Halton Council, and the Internet Service Provider (Halton) to ensure that systems to protect pupils are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Prevent

The Cavendish High Academy recognises its duty to protect our pupils from accessing terrorist and extremist material on the Internet. The School will therefore aim to do the following:

- Educate pupils on the appropriate use of social media and the dangers of downloading and sharing inappropriate material including that, which is illegal under the Counter- Terrorism Act.
- Ensure that pupils are unable to access any inappropriate Internet sites whilst using the school computers / laptops through the use of appropriate filtering, firewalls and security settings.
- Educate pupils through lessons and assemblies on the concepts of radicalisation and extreme ideology.
- Inform pupils on the importance of Internet Safety both through the ICT curriculum and PHSE education.

Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for 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.
- The senior management team should note that technologies such as mobile phones with wireless Internet access can bypass school

filtering systems and present a new route to undesirable material and communications.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones will be kept under review.
- 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.
- Staff will be issued with a school phone where contact with students is required.

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 'Staff Code of Conduct for ICT' before using any The Cavendish High Academy ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Secondary students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents/carers will be asked to sign and return a consent form.

Assessing the risks

- The Cavendish High Academy will take all reasonable precautions to prevent access to inappropriate material. However, due 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. Neither the school nor Halton Council can accept liability for any material accessed, or any consequences of Internet access.
- The Cavendish High Academy 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 by a senior member of staff.

- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (The Kent e-Safety Policy has a flowchart of responses to an incident of concern.)
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

- The Cavendish High Academy will liaise with local organisations to establish a common approach to e-safety.

Communicating e-Safety

Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used.
- Students will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety has been developed, and is based on the materials from CEOP.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must 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 senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters and the school Web site.
- The school will maintain a list of e-safety resources for parents/carers

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school will appoint an e-Safety coordinator.

- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

- The e-Safety Policy was revised by: … … … … ……..………………

- It was approved by the Governors on: … … ………………………….

- The next review date is (at least annually): … … …………………........