

# HIGHCLARE SCHOOL



## E-Safety Policy

### Introduction

The school, following government guidance, has written this e-safety policy. It has been agreed by senior management and approved by the school governing body.

The e-safety committee will review the e-safety policy and its implementation annually.

### Aims

The Internet is an essential element in our children's education, business and social interaction. We, as a school, aim to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils. The school intends to make such use normal practice for all staff and pupils.

This policy is consistent with our three school aims.

The school will ensure that:

- Pupils and their parents are provided with a copy of the acceptable use policy for ICT when the pupil joins the school.
- Pupils are regularly reminded of Internet safety rules
- The ICT programs of study teach Internet safety skills.
- Teachers in all curriculum areas using ICT to enhance teaching and learning are aware of, and teach about, Internet safety.
- Pupils in Key stages 2, 3, 4 and 5 are aware of, and comply with, relevant legislation when using the Internet, including:
  - Data Protection
  - Computer misuse
  - Copyright and intellectual property legislation.
- Pupils are clear about where to seek help and advice, should they experience any problems when using the Internet
- Staff, pupils and parents are aware that the school utilises surveillance software which records and tags any detected instances of inappropriate use of the Internet. This software also restricts Internet access by filtering. However, the growth of websites makes it impossible to guarantee that all offensive or dangerous materials will always be covered.
- Staff, pupils and parents are clear that the introduction of violent, degrading or sexual electronic materials into the school will not be tolerated.

## Actions the school is taking to ensure e-safety.

### **1 Teaching e-safety**

- School ICT lessons will cover Internet technologies and will teach e-safety throughout.
- Pupils will be taught what Internet use is acceptable, and what is not, and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

### **2 Communicating e-safety**

- Staff and pupils will be informed that Internet use will be monitored.
- E-safety rules will be communicated to pupils and parents annually during e-safety week.
- E-safety rules will be discussed with pupils at every possible opportunity.
- All staff will be given the e-safety policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Parents' attention will be drawn to the e-safety policy in newsletters, the school website and during e-safety week.

### **3 Monitoring Internet Activity**

#### **(i) Internet sites**

- The ICT team has a web surveillance facility available to them which incorporates web filtering.
- The ICT department, with help and advice from the Senior Leadership Team, will ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils discover an unsuitable site, it must be reported to the ICT department by email to [e-safety@highclareschool.co.uk](mailto:e-safety@highclareschool.co.uk) as soon as possible.

#### **(ii) Social Networking Sites**

- The school will block all access to social networking sites and instant messaging sites for pupils and staff.
- Pupils will be advised never to give out personal details of any kind and should only consider real people that they know, to be their friends online.
- Staff, pupils and parents will be advised to be very careful when using social networking sites outside of school. We draw attention to:-
  - Anything placed onto the Internet is effectively put into the public domain.
  - Whilst membership of sites can be restricted, it is not possible to control the way that other people use material that one gives access to.
  - Inappropriate comments about other staff or students made on a social network, instant message site or by email are unacceptable.

- Staff should not add current students to their social networking sites other than to systems set up by the school for teaching and learning that should have built in user identification and archiving. Students who make such invitations should be warned by pastoral staff about the inappropriateness of their actions.
- Staff should also be cautious of adding recent former students to their social networking sites as they may provide an indirect link to current students.
- Staff should also be cautious of adding current parents to their social networking sites as they may provide an indirect link to current students.

(iii) E-mail

- All email sent with a Highclare School email address will reflect upon the school and should be carefully written before sending, with the same attention as for a letter written on school headed paper.
- Materials that could be deemed offensive in any way should not be sent from a school email address.
- Staff may use their personal email at the school; staff should avoid communicating with pupils via their own personal email account. Staff should ensure that all correspondence to and from pupils is saved.
- Pupils are only permitted to use personal email in school during lesson time and morning break. This must only be for the sending or receiving of school work - *eg* homework to be printed off in school, or finished at home and with permission from the teacher in charge at the time
- Pupils must immediately tell a teacher if they receive offensive email at school.
- Pupils must not reveal personal details of themselves or others in e-mail communication.
- The forwarding of chain letters is not permitted whilst using email on the school network.

(iiii) Firewall and Anti-Virus

- The school has a 24/7/365 Antivirus software that updates continuously with the latest anti-virus definitions.

## **4 The School Website**

- Images of our students will only be included on the school website with the permission of the parents. given by signing the school contract when a pupil joins the school. There is an option in the contract for parents to opt out so that no identifiable images of their children will be used.
- There will be an e-safety section on our website that informs students and their families of simple steps they can take to ensure e-safety.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The website will be a means of inviting views of staff, pupils and parents through a secure email system or a VLE. This is not yet fully operational.

## **5 Data Protection Act**

- Personal Data will be recorded, processed, transferred and made available according to the Data Protection Act.
- The school recognizes that SIMS is an invaluable tool in the efficient running of the school. It is also an electronic data source and as such is subject to the full requirements of the Data Protection Act. To this end :-
  - SIMS must never be left running on an unattended PC.
  - Staff are reminded to either lock workstations or close SIMS down before leaving a PC.
- Staff must take extreme care not to transfer any sensitive data onto an external data storage device.

## **6 Managing Emerging Technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before school use is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff must not contact pupils using their own personal mobile phone.

## **E-safety Complaints**

Staff, pupils and parents will be informed of the complaints procedure.

### **Pupils**

- A senior member of staff will deal with complaints of Internet misuse.
- Complaints of a child protection nature must be dealt with in accordance with school protection procedures.
- Discussions with the police will be held in regard to handling potentially legal issues.

### **Staff**

- Any complaint about staff misuse must be referred to the head teacher.

### **Failure to comply**

#### Minor offences

Normal school procedures will be followed and alleged perpetrators will be dealt with fairly. Some pupils may not at first realise the seriousness of their actions such as passing on a copy of an offensive message to a friend. It must be made clear to the alleged offender that anyone who participates in the distribution of offensive material is supporting and reinforcing unacceptable use and behaviour.

### Serious offences

- In the opinion of the school the following breaches of the e-safety /acceptable use policy constitute serious offences:
  - Persistent bullying / harassment or racism
  - Serious breach of a person's privacy ( hacking of restricted network drives – use of video on mobile devices to cause embarrassment or offence)
  - Deliberate introduction of viruses into the school
  - Use of the school's infrastructure for any form of gambling
  - Blatant, deliberate exhibition of age-restricted materials.
  - Use of school's ICT infrastructure to procure illegal (or age limited) substances e.g. alcohol, drugs etc.
  - Possession of illegal images.

The discovery or reporting of a serious offence such as those described above will require immediate investigation by the Head of ICT and senior members of staff.

Where appropriate, the immediate involvement of the school's child protection officer will be sought.

For cases where pornography of minors, aggravated bullying, or the use of controlled substances is indicated the immediate involvement of the Police will be required.

<b>Written by:</b>	<b>Adopted by the Board:</b>	<b>Reviewed</b>	<b>Review Date:</b>
SR&E-safety committee Feb 2010 (amended September 2010)	June 2010	September 2011	July 2012