



## THE HESSE FEDERATION OF SCHOOLS



### E-SAFETY POLICY

**Effective Date:** November 2011

**Date of minuted approval by the governing body:** 20 July 2011

**Review Committee:** Personnel and Pay

**Review Date:** November 2012

#### **Rationale**

E-safety is a safeguarding issue, not an ICT issue. All people in a school, both adults and students have a duty to be aware of e-safety, to know the required procedures and to act on them. E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. The principles of the policy will be consistently applied to all forms of electronic communication.

Internet use is a part of the statutory curriculum and a necessary tool for staff and students. The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

The school's e-safety policy will operate in conjunction with other policies including those for Acceptable Internet Use, Behaviour for learning, Anti-Bullying, Curriculum, Data Protection and Security, the ERYCC Internet Policy and school email policy.

A designated member of SLT has responsibility for all e-safety matters.

#### **Use of the internet to enhance learning**

- The school internet access will be designed expressly for student use and will include filtering appropriate to the age of pupils.
- On entry to the school, ICT lessons will teach students what internet use is acceptable and what is not, and clear objectives for internet use will be given. Across the curriculum staff will guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- If staff discover unsuitable sites, the URL (address) and content must be reported to the Director of ICT
- The use of internet derived materials by staff and students will comply with copyright law with acknowledgement of sources as appropriate.

#### **Authorisation of internet access**

- A record of all students and staff who have been granted internet access will be held by the school and kept up-to-date
- Students will be informed that internet use is monitored and breaches of e-safety will be recorded and dealt with under the 'Behaviour for Learning' policy.

## **Risk Assessment**

- In common with other media some material via the internet is unsuitable for school students. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the *Computer Misuse Act 1990*.
- Access to websites that involve gambling, games (unless educationally relevant) or financial scams is strictly forbidden.
- The use of school equipment for file sharing copyrighted material is forbidden.
- Strategies to identify, assess and minimise risks will be reviewed regularly.

## **Managing filtering**

- The school will work in partnership with parents; the LA, DCFS and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- The Internet Gateway will be managed, maintained and monitored by Arvato IT services on behalf of the Local Authority
- The Headteacher or her representative will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation ([www.iwf.org.uk](http://www.iwf.org.uk)).
- In-house filtering will be appropriate to the age and curriculum requirements of the students and used in conjunction with school based 'policies' by which appropriate internet content is identified in advance of curriculum delivery.

## **Management of email**

- Students may only use approved email accounts on the school system, which they are aware are subject to monitoring.
- Access in school to students' personal e-mail accounts will be blocked.
- The forwarding of chain emails is prohibited.
- If a student receives offensive email, it must be reported immediately to a teacher, who may require it forwarding to an appropriate work email account to assist with further investigation.
- Students must not reveal details of themselves or others in email communication or via personal web space, such as address or telephone number, or make arrangements to meet anyone
- E-mail sent to an external organisation by a student must be authorised by a teacher before sending, in the same way as a letter on school headed paper, with a carbon copy sent to the authorising teacher.
- Personal email or messaging between staff and students/pupils is only permitted through [www.hesslehigh.net](http://www.hesslehigh.net) or [www.penshurstschool.net](http://www.penshurstschool.net) internal email facility and must be directly related to school matters. Both staff and students are aware that this system is monitored.

## **Managing website content**

- The point of contact on the website will be the school address, school email, fax and telephone number
- Photographs of students on the website will be carefully selected, students' full names will not be used with photographs or articles

- On an annual basis the school will seek permission of parents' and carers regarding the use of student photos in any publication
- The Headteacher or her representatives will take overall responsibility for the accuracy and appropriateness of content
- The copyright of all material is held by the school, or attributed to the owner where permission to use material has been obtained

### **Newsgroups E-mail lists and forums**

- Interest groups and forums will only be made available to students through the schools virtual learning environment.
- Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted.

### **Chat, Instant messaging, Blogs and social networking sites**

- Students will not be allowed access to public or unregulated chat rooms or social networking sites
- Permission may be granted by the Headteacher or her representative to access regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised as part of the learning objective.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.
- Staff must ensure that social networking sites are set to 'private' preventing access from students.
- No member of staff should be 'friends' with any student on a social networking site. eg Facebook, Myspace and Twitter.
- If a student has attempted to initiate an online communication through a social networking site or other online facility, the member of staff must inform their line manager immediately.
- No member of staff should put information on a social networking site regarding The Hesse Federation, including any members of the school community
- In addition any comment made by a parent relating to staff, school or students will be investigated as a serious incident. (see complaints policy).

### **Personal websites**

- When publishing material to websites and elsewhere, students should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.
- Should a member of staff design a website there must not be mention, either directly or otherwise, of The Hesse Federation or persons within the organisation.

### **Photographic, video and audio technology**

- When not in use, video conferencing cameras should be switched off and turned to face a wall.
- Care should be taken when capturing photographs or video to ensure that all students are appropriately dressed. It is not appropriate to use photographic or video devices in changing rooms or toilets.
- Staff may use photographic or video devices that belong to the school (including digital cameras and mobile phones) to support school trips and curriculum activities.

- Students must always seek the permission of their teacher before making audio or video recordings within school.

### **Managing emerging ICT applications**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of mobile phones by students for any purpose is not permitted during the school day.
- This use of any personal Bluetooth or wireless enabled device is not allowed to be used by students in school.

### **Personnel**

- All staff have a responsibility for **E-SAFETY**.
- All new staff will be taken through the key parts of this policy as part of their induction; copies of the policy are available in the policies area of the school website
- Staff should be aware that internet traffic is monitored and can be traced to the individual user.
- Staff development in safe and responsible internet use will be provided as required
- It is the responsibility of the individual member of staff to ensure that material contained in their files is fit for purpose and does not contain any offensive or copyright material
- Breaching the e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed

### **Maintaining the security of the ICT systems**

- The school systems will be reviewed regularly with regard to security; virus protection will be updated regularly
- Files held on the school's network will be checked regularly
- Unapproved system utilities and executable files will not be permitted in students' work areas or attached to email
- Staff are expected to check that any files that they propose to use in school are free from virus/spyware/malware

### **Handling misuse of the internet**

- Responsibility for handling incidents will be delegated to a senior member of staff
- The Headteacher and chair of Governors must be kept informed of any complaint regarding misuse by staff
- Students and parents will be informed that sanctions may be used to deal with misuse including, interview with a member of SLT, informing parents or carers and removal of internet or computer access for a period, which could ultimately prevent access to files on the system
- If an instance of severe misuse is suspected the police will be contacted to establish the legal position and discuss strategies, including advice on how best to preserve any possible evidence

### **Parental Support**

- A partnership approach with parents will be encouraged, including sessions on suggestions for safe internet usage and the issue of guidance leaflets
- Parents' attention will be drawn to the Acceptable Use policy in the Student Diary and asked to confirm their support by providing a signature.

- Additional guidance for parents will be provided in the Parents' Centre of the Virtual Learning Environment. Parents may also be referred to organisations such as Child Exploitation and Online protection (CEOP). A report abuse facility linking to CEOP is provided through the school website. Advice given by the school will be limited to e-safety and will not extend to technical advice
- Internet issues will be handled sensitively to inform parents without causing undue alarm

### **Monitoring**

- Records of student breaches of the policy will be kept in the student's file. The number and nature of breaches will inform the review of the policy.
- Records of staff breaches of the policy will be kept by the headteacher
- All records relating to breaches of the policy may be shared with legitimate agencies as necessary to ensure e-safety
- The governing body has a responsibility to monitor the effectiveness of the policy and to contribute to policy review

---

I have read the Hessle Federation E-Safety Policy and understand that I must adhere to it at all times.

Signed.....

Print.....

Date.....