

## E Safety Policy

*Holbrook aims to welcome everybody into our school. We will support all children and staff and provide challenging, fun and exciting learning activities. We will encourage everybody to learn, and learn from mistakes, to be independent and cooperative.*

### **Introduction**

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

### **Aims**

The Internet is now considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning. This e-safety policy considers the use of both the fixed and mobile internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- To use the Internet in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information systems.
- To ensure children are safeguarded whilst using ICT in school and are aware of how to protect themselves when using ICT
- To ensure all members of the school community are aware of the e safety policy and its implications.
- To make internet use as safe as possible within school
- To ensure pupils are aware of the guidelines for the acceptable use of the Internet and what is not acceptable.
- To ensure that curriculum activities involving the use of the Internet for gathering information and resources will develop pupil skills in locating and evaluating materials.
- To ensure that curriculum activities that involve the use of e-mail protect children and their personal information.
- To provide school information via a well maintained website which safeguards children.

### **Principles of Practice**

- Guidelines and details of the school e-safety policy will be made available to all members of the school community.
- All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school e-safety policy. Staff development in safe and responsible Internet use will be provided as part of the continuing professional development programme.
- Internet access in the school is provided via a broadband link through the SWGfL. Filtering appropriate to the age of the pupils is provided as part of this link. Virus protection is installed on all computers in school and automatically updated regularly. Portable media may not be brought into school without specific permission. Pupil access to the Internet will be by adult demonstration or directly supervised

access to specific, approved on-line materials. Instruction in responsible and safe use by pupils will precede Internet access.

- Guidelines for acceptable use will be clearly on display in all areas of the school where Internet access is available. All pupils will be given clear objectives when using the Internet. Where Internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the school.
- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- Pupils will be taught how to validate materials they read before accepting their accuracy. The use of search engines will be monitored. Other techniques for research will be developed through the use of school approved sites. Where materials gathered from the Internet are used by pupils in their own work, they will be taught to acknowledge the source of information used. The school will ensure that the use of Internet materials by staff and pupils complies with copyright law.
- All e-mail communications sent by members of staff that relate to the school will be through authorised, school controlled webmail accounts. The use of individual pupil personal accounts will be restricted to the teaching of email in ICT sessions Any e-mail sent to an external account will be authorised by the school, before sending, following the same procedure used for letters written on school headed notepaper. Pupils will never reveal personal details of any member of the school community in e-mail communications.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- The use of online chat rooms, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the pupils. The use of mobile phones will not be permitted during lessons or formal school time. This is to avoid the possibility of the sending of abusive or inappropriate text messages.
- The school website is maintained and kept up to date. The headteacher ensures that the content is accurate and appropriate to the needs of the school community. No personal information about any member of the school community will be published on the website. Written permission from parents or carers will be obtained before photographs of pupils or pupil names are published on the website. Only first names of pupils will be published and these will never be published in conjunction with photographs. Any photographs published will not allow individual pupils to be identified.
- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

### **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

## **Roles and responsibilities**

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

### **Governors**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee

### **Headteacher and Senior Leaders**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

### **E-Safety Coordinator:**

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

### **Technical staff**

The ICT Technician and ICT Co-ordinator are responsible for ensuring:

- that the school’s ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school’s networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator

### Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with pupils should be on a professional level
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### Designated person for child protection

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

### Students / pupils

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

### Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing the Student / Pupil Acceptable Use Policy
- accessing the school website pupil records in accordance with the relevant school Acceptable Use Policy.

### Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the SWGfL flow chart (see appendices) should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

## **Conclusion**

This policy should be considered alongside other relevant policies. It will be reviewed by the governing body as part of its schedule of policy review.

June 2009

Appendices to this policy

SWGfL acceptable use policy  
SWGfL internet safety protocol  
SWGfL reporting abuse guidelines  
SWGfL security policy