# E SAFETY POLICY

This Policy should also be read in conjunction with any relevant Jefferys Education Trust documentation/policies. Please ask if you need further information.

This policy applies to all people using school equipment. This includes teaching staff, administration staff, ancillary staff, site managers, students, pupils, parents and visitors. Hollybrook Infant School will ensure that every person to whom this policy applies is aware of its contents.

When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment. Parents will be requested to sign an e-Safety/internet agreement as part of the Home School Agreement. Any e-Safety issues or concerns will be taken to the ICT co-ordinator, Head teacher or the designated Child Protection Coordinator.

**Teaching and Learning**

Why the Internet and digital communications are important

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. Access to the Internet is a necessary tool for staff and an entitlement for pupils to give them experience of developments in Technology in the world around them.

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Inclusion in government initiatives
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Access to learning wherever and whenever convenient
- Exchange of curriculum and administration data with SCC and DCSF
- Provide opportunities for publishing and displaying work on a school web page

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

How Internet use enhances learning

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation, at an age appropriate level
- Internet access will be planned to enrich and extend learning activities.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- The school's internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils

How will pupils learn how to evaluate Internet content?

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.
- If staff or pupils discover unsuitable sites, the URL(address), time, date and content must be reported to the ICT co-ordinator to pass on to the internal IT technician and where appropriate to the school's e-safety officer.

**Managing Internet Access**

Information system security

- Virus protection will be updated regularly.
- The security of the school information systems and users will be reviewed regularly.
- Memory Keys and CD Roms may not be brought into school without a virus check.
- The ICT co-ordinator / network manager will review system security regularly.
- The school uses Broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system
- Pupils may send e-mail as part of planned lessons where whole-class or group e-mail addresses set up by the ICT Manager or Technician will be used. Pupils will not be given individual e-mail accounts
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
- In-coming e-mail should be treated as suspicious and attachments not opened unless the author is known
- Formal e-mails sent to an external organisation should be written carefully and authorised (by the Headteacher) before sending, in the same way as a letter written on school headed paper
- The forwarding of chain messages is not permitted.

Published content and the school's website

The contact details on the website should be the school address, office, email and telephone number. Staff or pupils' personal information must not be published. .

Publishing pupil's images and work

- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

Social Networking, Social Media and Personal Publishing

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- The school has an expectation that use of any social networking sites (e.g. Facebook, Twitter, Myspace) by staff does not bring the name of the school or any of its staff into disrepute. All staff are advised to set security and privacy filters on such sites appropriately to avoid making private details public. Staff should not accept contact from pupils via social networking sites.

Managing filtering

- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

**Staff internet responsibilities**

- A member of staff who flouts security advice, or uses email or the Internet for inappropriate reasons risks dismissal.

**Policy Decisions**

Authorising internet access

- At Key Stage 1, and during the Early Years Foundation Stage, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- All staff, administration staff, ancillary staff, site managers, students, parents and visitors must read and sign the "ICT acceptable internet use policy" before using any school ICT resources.

Assessing risks

- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor JET can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of the computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.
- All e-Safety complaints and incidents will be recorded by the school — including any actions taken.

Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Management of Cyber bullying

- Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- All incidents of cyber bullying reported to the school will be recorded.

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- Think then Click' Rules for Internet access will be posted in all classrooms.

How will the policy be discussed with staff?

- The e-Safety Policy will be formally provided to and discussed with all members of staff. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.

Policy written
20th December 2011
Review date December 2013
Reviewed by N Thorne & J Wood
Next Review due December 2015