e–Safety Policy

Introduction

The use of information and communication technologies (ICT) in this school brings great benefits. This document recognises that there are also safety issues surrounding electronic communications (e-Safety) and details strategies which will ensure appropriate, effective and safer use of electronic communications.

The e–Safety Policy is part of the ICT and Safeguarding Policies. The e–Safety Policy has been agreed by the Senior Leadership Group and approved by governors. It has been disseminated to all school staff and parents have been sent a summary together with guidance about e-Safety.

The school has appointed an e–Safety Coordinator. This person is the Designated Child Protection Coordinator as the roles overlap. Administrative support is provided by the school administrative staff and the ICT technician. The e–Safety Policy and its implementation will be reviewed annually.

The Age and Learning Difficulties of the Pupils

The pupils at the school cover a wide age range (3 to 11 years) and have a wide range of learning difficulties from moderate to severe to profound. For the majority of pupils independent use of electronic communications technologies is going to be impossible without a high degree of adult support. Yet a large minority of children are perfectly capable of learning the basic skills for electronic communications and discussions with their parents show that many use the Internet widely outside school. Therefore, it is essential that both they and their parents learn how to take care of their safety and security.

Many pupils are taught ‘how to keep safe’ especially in their later years at school and they must also be taught explicitly to link their existing knowledge of how to keep safe to the rules that will apply specifically to, for instance, internet use. Clear rules, supported by visual displays, are very helpful to these pupils.

Due to their age and learning difficulties, no child will be permitted access to electronic communications of any kind in school without close adult supervision.

Uses of the Internet

The school has a duty to provide pupils with quality Internet access as part of their learning experience. The benefits for staff and pupils of using the Internet in school include:

- access to world-wide educational resources including museums and art galleries;
- access to banks of photos, pictures and symbols and moving images that can be used to enhance teaching and learning
- connections to other schools in the UK;
- educational exchanges between pupils world-wide;
- social and leisure use at home;
- 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;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the local authority;
- access to learning wherever and whenever convenient.

Safe use of the Internet in learning

As noted above, no child will be permitted access to the Internet in school without close adult supervision. However, many pupils have the capability to learn basic digital literacy skills to communicate with others via the Internet. Therefore, these pupils will be taught what Internet use is acceptable and what is not.

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

- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to appropriate on-line activities that will support the learning outcomes planned for them given their age and learning difficulties.
- Pupils will be educated in the effective use of the Internet, including the skills of knowledge location and retrieval.

The quality of information received via the Internet is variable and everyone needs to develop critical skills in selection and evaluation. Given the pupils' learning difficulties, teachers will find it difficult to teach them to be critically aware of the materials they access. Therefore, it is essential that teachers carefully evaluate on-line materials before using them in teaching.

Managing Information Systems

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for the network use. Flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- The server is located securely and physical access restricted.
- The server operating system is kept up to date.
- Virus protection for the whole network is installed and regularly updated.

Wide Area Network (WAN) security issues include:

- All Internet connections are arranged via the Yorkshire and Humberside Grid For Learning (YHGFL) and the council's IT team to ensure compliance with the security policy.
- Broadband firewalls prevent unauthorised access.

School practice is that:

- Virus protection is updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media (e.g. laptops) may not used without specific permission followed by a virus check.
- Unapproved software is not allowed to be used in school or on school laptops used at home.
- Files held on the school's network will be regularly checked.

E-mail

E-mail use can bring significant educational benefits and interesting projects between schools. Security is ensured by the following strategies:

- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes
- Personal details about pupils or others must not be revealed in email communication.
- Due to the possibilities of identification by unsuitable people, e-mail accounts will not be not provided for individual pupils. Whole-class email addresses are used.

Management of the school website

The school has a website that celebrates pupils' achievements, promotes the school and publish resources for parents.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- The contact details on the website should be only the school address, email and telephone number.
- Staff or pupils' personal information must not be published.

Publication of pupils' images on the website and in newsletters

Still and moving images add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

The publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.
Strategies include:

- Use will be made of relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace “passport style” photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils’ work or of a team activity.

- Pupils in photographs should be appropriately clothed.
- Images of a pupil should not be published without the parent’s or carer’s written permission. The school will seek permission to publish images of work or appropriate personal photographs on entry.
- Images that include pupils will be selected carefully and will not provide material that could be reused.
- 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

The Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

Pupils do not have the skills or opportunities for social networking in school. Parents are encouraged to control this activity at home.

- Staff are made aware of the potential risks of personally using social networking sites. They are asked to consider the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.
- Staff must not access social media and social networking sites in school using school equipment.
- Staff are advised never to give out personal details of any kind which may identify them and the school where they work, e.g. real name, address, mobile or landline phone numbers, school, email addresses, full names of friends/family, specific interests and clubs etc.
- Staff are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff are advised not to publish specific and detailed private thoughts, especially those that may be considered hurtful or defamatory.

Filtering

The YHGFL uses an industry-standard filtering system considered appropriate by the local authority. Unsupervised Internet access is not permitted for any pupil. Staff might need to research all kinds of areas and require less restricted use temporarily

- The school will work with the local authority’s IT Team to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.
- The school’s broadband access includes filtering appropriate to the age and maturity of pupils.

- Any material that the school believes is illegal will be reported to appropriate agencies.

Videoconferencing

Videoconferencing enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many uses in education. Currently, it is not used in school but its use at a future date is envisaged as a possibility.

- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing by pupil should be supervised closely.
- Parents and carers should agree for their children to take part in videoconferences.
- Only the SLG, the ICT technician and office administrative staff should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Preparation and evaluation are essential to the whole activity.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

Personal data protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 (“the Act”) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up- to- date
- Held no longer than is necessary
- Processed in line with individual’s rights
- Kept secure
- Transferred only to other countries with suitable security measures.

In this school, personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

All pupils may have Internet access at school, but only under close supervision. Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on line materials. Parental permission will be required for Internet access in all cases as new pupils join.

All staff must read and sign the ‘Staff Information Systems Code of Conduct’ before using any school ICT resource.

Risks assessment

Many emerging communications technologies offer the potential to develop new teaching and learning tools. The school will keep up to date with new technologies as they emerge. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

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 the local authority can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will regularly audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Dealing with e–Safety complaints

Parents, teachers and pupils should know how to use the School’s complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

A minor transgression of the rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions will be required, linked to the school’s

disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator who is the e–Safety Coordinator.
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.

All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

Cyberbullying

'Cyberbullying' is the use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone. The use of cyberbullying by pupils at thi school is highly improbable due their age and learning difficulties. Nevertheless, it constitutes a risk, no matter how remote.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.

Cyberbullying (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 cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Parent/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

Learning Platforms and learning environments

The school is moving to develop a learning platform (LP) by 2012. An effective learning platform will offer a wide range of benefits to teachers, pupils, parents as well as support management and administration. It can enable pupils and teachers to collaborate in and across schools, can share resources and tools for a range of topics, create and manage digital content and pupils can develop online and secure e-portfolios.

The school will follow the recommendations of the local authority in adopting a LP and when it is running there will be careful monitoring by SLG.

- SLG and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Staff will be advised on acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.

- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Any concerns with content will be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LP for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement.

A visitor may be invited onto the LP by a member of the SLG. In this instance there may be an agreed focus or a limited time slot.

Communication Policy

Pupils:

Pupils are involved in reviewing the school e–Safety Policy through the school council. As pupils' perceptions of the risks will vary; the e–Safety rules may need to be explained or discussed.

The school will display posters with the e–Safety rules in every room with a computer to remind pupils of the e–Safety rules at the point of use.

E–Safety will be taught as an ICT lesson activity, as part of the Personal, Social and Health Education programme and whenever pupils are using the internet.

All users will be informed that network and Internet use will be monitored.

Staff:

If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Staff who are provided with devices by the school which may be accessed outside of the school network must follow the guidance on their use which is detailed separately.

Staff must be made aware of their responsibility to maintain confidentiality of school information.

Induction of new staff should include a discussion of the school e–Safety Policy.

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.

Staff that manage filtering systems or monitor ICT use will be supervised by the SLG and have clear procedures for reporting issues.

Staff training in safe and responsible Internet use both professionally and personally will be provided.

Parents:

Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website. They will be requested to sign an e–Safety/internet agreement.

Information and guidance for parents on e–Safety will be made available to parents in a variety of formats. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Interested parents will be referred to organisations listed in section "e–Safety Contacts and References."

This policy was adopted on: ______________________and minuted at the Governing

Body Meeting held on ___________________

e-Safety Contacts and References

Becta: *www.becta.org.uk/safeguarding*
CEOP (Child Exploitation and Online Protection Centre*):* *www.ceop.police.uk*
Childline: *www.childline.org.uk*
Childnet: *www.childnet.com*
Click Clever Click Safe Campaign: *http://clickcleverclicksafe.direct.gov.uk*
Cybermentors: *www.cybermentors.org.uk*
Digizen: *www.digizen.org.uk*
Internet Watch Foundation: *www.iwf.org.uk*
Kidsmart: *www.kidsmart.org.uk*
Teach Today: *http://en.teachtoday.eu*
Think U Know website: *www.thinkuknow.co.uk*
Virtual Global Taskforce — Report Abuse: *www.virtualglobaltaskforce.com*