HOLY TRINITY

Church of England Primary School

E-Safety Policy

Introduction

Internet use is part of the statutory curriculum and is a necessary tool for learning. It is a part of everyday life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Pupils use the Internet widely outside of school and need to learn how to evaluate Internet information and to take care of their own safety and security.

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 functions.

Summary of the key points of this policy

The Internet is a vital tool in our school's aim of delivering a rich, balanced and exciting curriculum. With more and more children accessing the Internet outside school and as part of a social context, we have a duty to support pupils in becoming competent and safe users of this technology. The Internet brings many benefits to education for both pupils and staff. Pupils need to learn the importance of checking reliability and accuracy of information they obtain from digital sources.

Security of the school's information systems will be regularly reviewed, and pupils will be taught the information that can be safely shared with others. Anonymous images of pupils will be used where appropriate, and with parental permission. Although social networking does not feature as part of our curriculum use, pupils will be taught how to use it safely and appropriately as part of their e-Safety education. Internet access is filtered to ensure that content is appropriate to the age and maturity of the pupils, and new technologies are carefully assessed for educational benefits before their introduction into school. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Pupils and parents receive an Acceptable Internet Use for Pupils Policy and are requested to complete the Internet Parent/Guardian Permission Form and return to school.

Although all reasonable precautions are taken the school does not accept liability for any consequences resulting from Internet use. Complaints about Internet misuse are handled as part of the school's complaints procedure. All incidents are recorded.

Teaching and Learning

1. **Why is Internet use important?**

   Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and

social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

2. How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for all staff, including sharing good practice;
- improved access to technical support;
- exchange of curriculum and administration data;
- access to learning wherever and whenever convenient.

3. How can Internet use enhance learning?

The school's Internet use will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Access levels will be reviewed to reflect the curriculum requirements, age and maturity of pupils. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

4. 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 now plays a larger role in the teaching/learning within every subject.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will use age-appropriate tools to research Internet content.

Managing Information Systems

1. How will information systems security be maintained?

The security and capacity of the school information systems and users will be reviewed regularly. All servers, wireless systems, network components and cabling are securely located and physical access is restricted.

The school computer network is regularly checked for viruses, Malware and Spyware. Virus protection is installed on all school computers/laptops and configured to receive regular updates. Staff will be provided with encrypted memory sticks.

Sensitive data, including that sent over the Internet or taken off site, will be password protected. All staff and pupils will be reminded to follow the agreed format for creating password's and the need to keep passwords secure. Passwords are changed on a regular basis. All memory sticks are ebncrypted.When a member of staff or pupil leaves the school their access to the computer network and e-mail is terminated immediately. Software, including browser tool bars, should not be downloaded or installed on school computers/laptops without prior consent from the Head Teacher. An up to date record of all appropriate licences for all software is kept within school.

2. How will filtering be managed?

The school will ensure that the computer network is as safe and secure as possible. We will work with Advantex (our technology provider) to regularly review and improve our system security. Our filtering system offers a high level of protection that meets Internet Watch Foundation (IWF). The school uses Sonic Firewall, all inappropriate internet sites are locked.However, the nature of the Internet makes it impossible to ensure that all inappropriate material is blocked.

Children will always be supervised by a member of staff when using computer equipment in school.

If staff or pupils discover unsuitable content when using the internet/email, the URL/email must be reported to the Head Teacher who will follow the agreed school procedures.

3. How will remote access be maintained?

When using any type of remote access to school data, staff are required to adhere to the school agreed password and encryption policy. All staff will sign an AUP regarding access to school data. Third parties will only be given remote access with prior authorisation from the Headteacher and governing body.

4. How should personal data be protected?

All data should be kept secure and staff will be informed of what they can and cannot do with data. Personal/sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Under the Data Protect Act (1998) all schools must comply with the eight enforceable principles of good practice. Data must be; Fairly and lawfully processed, Processed for limited purposes, Adequate, relevant and not

excessive, Accurate, Not kept longer than necessary, Processed in accordance with the data subject's rights, Secure and Not transferred to other countries without adequate protection.

5. **How will e-mail be managed?**

Pupils may only use the approved e-mail accounts set up by the school. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult. Pupils must immediately tell a teacher if they receive offensive e-mail. Access, in school or via school laptops, to external personal e-mail accounts is not permitted.

Staff and pupils are made aware, through the AUP, that all e-mail communications may be monitored.

Email users within school are made aware, through training, that emails are covered by the Data Protection Act (1990) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

Staff are made aware that information stored on school equipment may be subject to release to the public at large under the Freedom of Information Act (FOI). Communications should be kept professional at all times. School information stored on personal devices may also be subject to FOI.

Read the Acceptable Use Agreement for e-mail for more detailed guidance.

6. **How will published content be managed?**

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

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright. The school website will adhere to the statutory requirements as set out by the DfE.

7. **Can pupils' images or work be published?**

Images that include pupils will be selected carefully and will not provide material that could be reused. Pupils' full names will never be published in association with photographs. Written permission from parents/carers will All staff/pupils are educated about the risks of taking, using, sharing, publishing and distributing digital media.

Photographs, images and videos are regarded as personal data under the Data Protection Act (1998). Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

8. How will social networking, social media and personal publishing be managed?

The school will block access to social networking sites.
As part of their e-Safety education, pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include: real name, address, phone numbers, school, IM and e-mail addresses, friends names, etc.

Pupils are educated not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location, e.g. house number, street name or school.

Pupils should be educated on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged only to invite known friends and deny access to others.

As part of the Acceptable User Policy, staff are asked to ensure that any personal social networking sites / blogs that they create or actively contribute to are not confused with their professional role. They are asked not to create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring their professional role, the school, or the Church, into disrepute.

Staff are made aware that images of other staff or pupils are not to be posted on third party websites (Facebook, Twitter, etc) as often the rights to the images transfer to the third party and may be sold on or distributed to advertisers without consent.

9. How will mobile phones, personal devices and other emerging technologies be managed?

Staff will be made aware, in the AUP, that they are responsible for safeguarding school ICT equipment (such as laptops) and should take all precautions necessary to prevent theft, loss or damage of such items and prevent unauthorised access.

Removal of mobile technology from school premises is only permitted with prior authorisation from the Headteacher and the equipment taken is logged. It is understood that any equipment taken is for school use only.
Our school policy is that mobile phones / handheld devices are not brought into school by pupils, but in exceptional circumstances they may be permitted and held securely in the classroom.

Staff are not permitted to use mobile phones during lesson times, unless prior consent is given from the Headteacher. Staff can use their mobile phones on designated break times away from any children

The school is responsible for ensuring all equipment is protected. As well as encrypting devices, training for staff should be provided to state how equipment should be transported and stored when off site (especially if it contains personal or confidential information).

Policy Decisions

How will Internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications. All staff must read and sign the Acceptable Use Policy before using any school IT resource. Parents are asked to sign and return a consent form for pupil Internet access.

How will risks be assessed?

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 council can accept liability for the material accessed, or any consequences resulting from Internet use. The school will regularly audit IT to ensure that the e-Safety policy is adequate and its implementation appropriate.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

How will e-safety complaints be handled?

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 – and kept for reference. Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice. Discussions will be held with South Tyneside's Children's Safeguarding Board to establish procedures for handling potentially illegal issues for which the police will need to be involved.

Communication Policy

1. **How will the policy be introduced to pupils?**

   All users will be informed that network and Internet use will be filtered. Pupils will be made aware through the ICT curriculum about the importance of safe and responsible internet use. Pupil instruction in responsible and safe use should precede all Internet access. Particular attention will be given where pupils are considered to be vulnerable.

2. **How will parents' support be enlisted?**

Information and guidance for parents on e–Safety will be made available to parents in a variety of formats. Parents' attention will be drawn to the School e–Safety Policy in newsletters and on the school website.
All e safety incidents are reported to the Headteacher, recorded and reported to Advantex who manage this on our behalf.