E-safety Policy and Acceptable ICT Use Agreement

CHALLENGE · INSPIRE · SUCCEED

September 2019

Headteacher: *K Trethewy*

Chair of Governors: *C Hammond*

Thorpe Primary School welcomes our duties under the Equality Act 2010 to eliminate discrimination, advance equality of opportunity and foster good relations in relation to age (as appropriate), disability, ethnicity, gender (including issues of transgender, and of maternity and pregnancy), religion and belief, and sexual identity.

We welcome our duty under the Education and Inspections Act 2006 to promote community cohesion.

We recognise that these duties reflect international human rights standards as expressed in the UN Convention on the Rights of the Child, the UN Convention on the Rights of People with Disabilities, and the Human Rights Act 1998.

Content

1. Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing.

This policy highlights the need to:

1. Educate pupils about the benefits and risks of using technology;
2. Provide safeguards and awareness for all users

All staff and volunteers within school should:

1. Make reference to the Staff Code of Conduct, alongside this policy
2. Read and follow the Acceptable ICT Use Agreement (Appendix A)
3. Sign to say they will work within these frameworks

2. Teaching and learning

Why Internet use is important:

- The Internet is an essential element in 21st century 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
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils

Internet use will enhance learning:

- The school Internet access will include filtering appropriate to the age of pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content:

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Staff will consider key safety issues relating to teaching and learning (Appendix 2)

3. Managing Internet Access

3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be updated regularly

3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate

3.4 Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site

3.5 Social media

- The school will block/filter access to social networking sites
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils Staff and volunteers must not give their personal contact details such as home or personal phone numbers, e-mail address or social networking details to pupils unless the need to do so is agreed in writing with senior management.
- It is recommended that staff ensure that all possible privacy settings are activated to prevent pupils from making contact on personal profiles and to prevent students from accessing photo albums or other personal information which may appear on social networking sites.
- Staff must not have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites. Staff are advised not to have any online friendships with any young people under the age of 18, unless they are family members or close family friends. Staff are advised not to have online friendships with parents or carers of pupils, or members of the governing body/trustees. Where such on line friendships exist, staff must ensure that appropriate professional boundaries are maintained.
- Staff are personally responsible for what they communicate in social media and must bear in mind that what is published might be read by us, pupils, the general public, future employers and friends and family for a long time. Staff must ensure that their on-line profiles are consistent with the professional image expected by us and should not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which may be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct which may be dealt with under the school's disciplinary procedure. Even where it is made clear that the writer's views on such topics do not represent those of the school, such comments are inappropriate.

3.6 Photography, Videos and other Creative Arts

Many school activities involve the taking or recording of images. This may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. The General Data Protection Act 2018 affects the use of photography. An image of a child is personal data and it is, therefore, a requirement under the Act that consent is obtained from the parent of a child before any images are made such as those used for school web sites, notice boards, productions or other purposes.

Staff should remain sensitive to any pupil who appears uncomfortable and should recognise the potential for misinterpretation. It is also important to take into account the wishes of the child, remembering that some children do not wish to have their photograph taken

Adults must only use school equipment provided or authorised by the school to make/take images and should not use mobile telephones or any other similar devices to make/take images.

The following guidance must be followed:

- if a photograph is used, avoid naming the pupil
- if the pupil is named, avoid using the photograph
- photographs/images must be securely stored and used only by those authorised to do so.
- be clear about the purpose of the activity and about what will happen to the photographs/images when the lesson/activity is concluded
- ensure that a senior member of staff is aware that the photography/image equipment is being used and for what purpose.
- ensure that all photographs/images are available for scrutiny in order to screen for acceptability
- be able to justify the photographs/images made
- do not take photographs in one to one situations.
- do not take, display or distribute photographs/images of pupils unless there is consent to do so.

3.7 Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

3.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Act 2018.

4.0 Policy Decisions

4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials

4.2 Assessing risks

- 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 school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective

4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

5. Raising awareness

5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year
- Pupils will be informed that network and Internet use will be monitored.

5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

5.3 Enlisting parents' support

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

Monitoring & Reporting

Our service provider, E2BN will monitor and audit the use of the service to see whether users are complying with this policy.

Any potential misuse identified by E2BN will be reported to the connected establishment and/or relevant organisation.

Where use contrary to this policy is suspected, users should apply local procedures for the reporting of the matter. Notification of any incidents to E2BN should be by the use of e-mail to abuse@e2bn.org

Appendix 2

Acceptable Use Agreement

Introduction

The purpose of this agreement is to ensure that staff are fully aware of their professional responsibilities when using information systems within school. The policy aims to ensure that information systems, including the internet, is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk.

Use of Internet facilities

The school expects all users to use the Internet responsibly and strictly according to the following conditions (for the purposes of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups):

- You must not send or receive materials or data, which:
    - Is in violation of any law or regulation
    - Is defamatory, offensive, abusive, indecent, or obscene
    - Constitutes harassment
    - Is in breach of confidence, privacy, trade secrets
    - Is in breach of any third party Intellectual Property rights (including copyright)
    - Is in breach of any other rights or has any fraudulent purpose of effect.
- You are prohibited from storing, distributing or transmitting or permitting the storage distribution or transmission (whether intentionally or otherwise) of, any unlawful material through the Service.
- You may not post, upload or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on school servers without the consent of the copyright holder.
- Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Such files must never be transmitted or redistributed to third parties without the express permission of the copyright owner.
- If inappropriate material is accessed accidentally, users should immediately report this so that this can be taken into account in monitoring.
- Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:
    - Images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
    - Adult material that potentially breaches the Obscene Publications Act in the UK

- Material which is criminally racist in the UK

- Users shall not:
  - Use computers in school for running a private business
  - Reveal or publicise confidential or proprietary information, which includes but is not limited to financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships
  - Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the Internet;
  - Send e-mail to any user who does not wish to receive it
  - Use any email address that you are not authorised to use

Appendix 2: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.