THORPEPARK

E-SAFETY POLICY

Date policy reviewed: February 2018
Date previously approved by Governing body: 11th October 2016
Date approved by the Governors: 24th February 2018
Person responsible for this policy: Melanie Legg

VERSION 2.0

Thorpepark internet and E-Safety policy statement

Teaching and learning

Why the Internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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 be monitored for pupil use and 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 its use.

Pupils will learn about computer networks including the internet and how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration.

Pupils will also be taught how to use search technologies effectively, appreciating how results are selected and ranked, and be discerning in evaluating digital content

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 will be taught how to report unpleasant internet content.

Managing internet access

Information system security

School ICT systems security will be reviewed regularly within the school and by Primarytec. Virus protection will be updated regularly. Security strategies will be discussed with the internet provider.

E-mail

Pupils may only use the approved itslearning e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. E-mails from pupils to external bodies are presented and controlled by the internet filter, the class teacher or the admin staff.

Published content and the school web site

The head teacher and computing coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate. Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Staff should consider using group photographs rather than full face photos of individual children. Pupils full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use. 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, their friends or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

The school will work with Primarytec to ensure systems to protect pupils are continually reviewed and improved. If staff or pupils view unsuitable on-line materials, the site must be reported to the e-Safety Coordinator. Senior staff, the e-safety co-coordinator and Primarytec will ensure that regular checks are made to the filtering methods in order they are appropriate, effective and reasonable.

Radicalisation procedures and monitoring

Serious incidents involving radicalisation have not occurred at Thorpepark to date. However, it is important for us to be constantly vigilant and remain fully informed about issues that affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/ Safeguarding Coordinator).

Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and students.

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. The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

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

Policy Decisions

Authorising Internet access

All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised

access to specific, approved on-line materials. At Key Stage 2, access to the Internet will be directly supervised access to specific, approved on-line materials.

On entrance to the school, parents will be asked to read, sign and return a Rules for Responsible Internet Use consent form.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Hull City Council can accept liability for any material accessed, or any consequences of internet access.

Thorpepark audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

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;
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and Internet use will be monitored and appropriately followed up. A programme of training in e-Safety will be developed. E-Safety training will be embedded within the ICT scheme of work.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained. Staff must be informed that network and internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils, safe search engines include

- bing.com;
- kids.yahoo;
- askkids.com;
- pawsexplore.com.

Teachers and children are not to use the search engine Google to search for images.

All USBs and mobile storage devices used within the school and contain children's personal data or assessment information must be encrypted.

Mobile technology

All mobile technology will be password / code protected to comply with safe guarding regulations. They will be kept in a locked cabinet at the end of each day. The key for the tablet trolleys will be kept by the computing coordinator and all staff that require access will sign the key in and out.

Enlisting parents' and carers' support

Parent and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school web site. The school will maintain a list of e-safety resources for parents and carers. The school will ask all new parents and carers to sign the parent/pupil agreement when they register their child with the school.