Ghyll Royd School and Pre-School
A foundation for life

E-Safety Policy

Policy Leader: Hadley Nicholson
Reviewed Date: January 2024
Review Date: January 2026

Ghyll Royd School and the Pre-School (Early Years Foundation Stage) is committed to safeguarding and promoting the welfare of young children and expects all staff and volunteers to share this commitment. Safeguarding at Ghyll Royd School and in the Pre-School is everyone's responsibility and everybody is able to make a referral to children's social care if needed.

Policy Statement

The E-Safety Policy should be read in conjunction with other school policies including those for ICT, Anti Bullying and for Child Protection. Our E-Safety Coordinator is the Deputy Headteacher. This may also be the Designated Safeguarding Lead as the roles overlap. The E-Safety Co-ordinator is not a technical role.

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 designed expressly for pupil use and will include filtering (Smoothwall) 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 shown how to publish and present information to a wider audience. 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 the importance of cross-checking information before accepting its accuracy.

E-mail and Teams.

Pupils may only use approved 365 e-mail and Teams accounts on the school system. Child friendly software is used in KS2 and each child is logged in by their own login password. Pupils must immediately tell a teacher if they receive offensive e-mails or Teams communications. 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. The school should consider how e-mail from pupils to external bodies is presented and controlled. The forwarding of chain letters is not permitted.

Published content and the school web site

Staff or pupil personal contact information will not be published. No personal details are given on pupils. The contact details given online should be the school office. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. 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 web site or social media. Work can only be published with the permission of the pupil and parents/carers. Pupil image file names will not refer to the pupil by name. Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing

The school will control access to social networking sites and consider how to educate pupils in their safe use. 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. Pupils will be advised to use nicknames and anonymous profile pictures, (avatars) when using social networking sites.

Managing video conferencing & webcam use

Online conferencing should use the educational broadband network to ensure quality of service and security. Pupils must ask permission from the supervising teacher before making or answering a conferencing call. Conferencing and webcam use will be appropriately supervised for the pupil's age.

Managing filtering

The school will work with the School's IT provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, the site 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.

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. Mobile phones will not be used in school by the children or in the presence of children by the staff. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering are not allowed in school.

Protecting personal data

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

Assessing risks

The school will take all precautions to prevent access to inappropriate material. 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 and effective.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by the SLT. 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 safeguarding procedures. Pupils and parents will be informed of the complaints procedure (see schools Complaints Policy). Pupils and parents will be informed of consequences for pupils misusing the Internet.

Introducing the e-safety policy to pupils

E-Safety SMART rules will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will not work on the internet unsupervised. Pupils will be informed that network and Internet use will be monitored and appropriately followed up. A programme of training in e-Safety has been developed, based on the materials from CEOP. E-Safety training will be embedded within the Computing scheme of work and the Personal, Social, Health and Education (PSHE) curriculum.

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. The IT provider that manages filtering systems or monitor ICT use will be supervised by SLT and work to clear procedures for reporting issues. Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website. The school will maintain a list of e-safety resources for parents/carers and host an e-safety evening for parents each year.