Helmsley Community Primary School – Internet Usage Policy

Internet access is planned to enrich and extend learning activities. The school has acknowledged the need to ensure that all pupils are responsible and safe users of the Internet and other communication technologies. An e-Safeguarding Policy has thus been drawn up to protect all parties and rules for responsible internet use will be displayed where users access the internet. An E – Safeguarding coordinator works alongside the Child Protection Officer to ensure that internet safety remains a high priority. Although the school offers a safe online environment through filtered internet access we recognize the importance of teaching our children about online safety and their responsibilities when using communication technology.

Section 1 - Student Internet Access

1. All students will have access to Internet resources through the classroom workstations, tablets and the ICT suite.
2. Students will have e-mail access only under direct teacher supervision, using the classrooms e-mail account. All e-mail to students is to be screened.
3. Children are to be supervised at all times when accessing the Internet.

Use of school computers by pupils must be in support of the aims and objectives of the National Curriculum.

Acceptable Uses

1. The use of email and computer conferencing for communication: between colleagues, between pupils(s) and teacher(s), between pupil(s) pupil(s), between schools and industry.
2. Use of the Internet to investigate and research school subjects, cross-curricular themes or topics related to social and personal development.
3. Use of the Internet to investigate careers and Further and Higher education.
4. The development of pupils' competence in ICT skills and their general research skills.
5. In support of the production of work to develop learning across all areas of the curriculum.

Unacceptable Uses

The following uses are considered unacceptable:

1. Personal Safety - Students will not post personal contact information about themselves or other people. Personal contact information includes address, telephone, etc.
2. Illegal Activities - Students will not attempt to gain unauthorized access to any other computer system through or go beyond the school authorized access account. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".
3. System Security - Students are not to download programs or files without seeking permission from the IT subject leader first.
4. Inappropriate Language - Restrictions against Inappropriate Language apply to public messages, private messages, and material posted on Web pages.

5. Students will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful languages
6. Students will not post information that could cause damage or a danger of disruption.
7. Students will not engage in personal attacks, including prejudicial or discriminatory attacks.
8. Students will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending them messages, you must stop.
6. Plagiarism and Copyright Infringement
7. Teachers need to be aware of copyright laws with regards to information on the World Wide Web. Teachers must enforce these laws with regard to student material taken form the web.

Section 2 – Staff

Staff Internet Access

1. All staff will have access to Internet resources through the ICT Suite, Classrooms and the staffroom.
2. Staff are assigned a helmsley.n-yorks mail account for personal professional correspondence. The school e-mail accounts are to be used for official correspondence only. Staff are to respect each-other's privacy with regards to e-mail as they would any other form of correspondence.
3. All staff will log on to the computer network through their individual log on with password.
4. When finished all staff will log off their account.
5. If a computer is found to be logged on to another member of staff's account, Logging off must be completed and the user will log on to their own account before any work is continued.

Unacceptable Uses

The following uses are considered unacceptable:

1. Illegal Activities - Staff will not attempt to gain unauthorized access to any other computer system through or go beyond the school authorized access account. This includes attempting to log in through another person's account, sending e-mail from another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".
2. System Security – Staff are to seek advice when downloading programs or files, from the IT coordinator.
3. Inappropriate Language - Restrictions against Inappropriate Language apply to public messages, private messages, and material posted on Web pages. When acting in an official capacity on behalf of the school, or using the school e-mail accounts, the following points are to be noted.
4. Staff will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
5. Staff will not post information that could cause damage or a danger of disruption.
6. Staff will not engage in personal attacks, including prejudicial or discriminatory attacks.
7. Staff will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending them messages, you must stop.
8. Staff will not knowingly or recklessly post false or defamatory information about a person or organization.

Respect for Privacy

1. Staff will not repost a message that was sent to you privately without permission of the person who sent you the message.
2. Staff will not post private information about another person.
3. Plagiarism and Copyright Infringement - Staff needs to be aware of copyright laws with regards to information on the World Wide Web. The same precautions are to be taken with information from the World Wide Web as those of print. When in doubt, contact the webmaster of the site you seek information from.
4. Inappropriate Access to Material - You will not use the school computers to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). A special exception may be made for hate literature if the purpose of your access is to conduct research.
5. Due Process - school will cooperate fully with local, county, or national officials in any investigation related to any illegal activities conducted through the school system.
6. Working with Children - When working with children on the Internet, staff are to supervise children at all times. If children are observed to be accessing inappropriate materials, there are two courses of action.
    a. Where children deliberately access inappropriate material
    Student is to be removed from computer and all computer privileges are suspended for one week. Subsequent offences will occur heavier penalties, to be decided by the Head of School in conjunction with the IT Subject Coordinator.
    b. Where children inadvertently access inappropriate material, the site is to be turned off immediately.
    c. All incoming and outgoing e-mail written by students is to be screened by the teacher. Inappropriate mail is to be deleted/not sent. Staff are to encourage responsible access at all times.

Section 3 - School Web Site

1. The Helmsley Community Primary School web site is located at **http://www.helmsley.n-yorks.sch.uk**. The software package used to edit and maintain the site is Webanywhere, School Jotter 2.

Update of Site

1. Ideally, the website should be updated at least once per week. Once per month is a recommended minimum. Items to go on the website include children's best work, upcoming events, photos of events, cultural information and other items deemed to be newsworthy.
2. The Head of School and IT Subject Leader are responsible for updating the site - however, other staff are encouraged to contribute. Training is to be negotiated with the administration staff and the IT Coordinator
3. At the beginning of each year or enrolment during the year all parents and caregivers will be asked to give permission to use their child's work/photos on the school web site.
4. Photographs of children will only be posted on the internet as part of a group of children. No child will be named with a photograph.
5. Before posting student work on the Internet, a check needs to be made to ensure that the child's caregivers have given permission for work to be displayed.

Section 4 – Auditing of Internet Access and Use

1. All users of the computer network need to be aware that the computer system may be independently audited at an undisclosed time. A record of the audit will be provided to the Subject Coordinator and Head of School.

Last Review

Staff March 2019

Next Review

Spring Term 2020

Supplementary Guidance for All Users

North Yorkshire LA supports the implementation and sharing of effective practices and collaborative networking across the LA as well as nationally and internationally

Staff are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others in the education world. Electronic information-handling skills are now fundamental to the preparation of citizens and future employees in the Information Age. Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use, and provide guidance and instruction to pupils in the acceptable use of the Intranet/Internet.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.

Pupils are responsible for their good behaviour on the school networks, just as they are on and off school premises. While the use of information and communication technologies is a required aspect of the national Curriculum, access to the Intranet/Internet is a privilege – not a right. It will be given to pupils who act in a considerate and responsible manner, and may be withdrawn if they fail to maintain acceptable standards of use.

Staff should ensure that pupils know and understand that, in addition to the points found under Online activities which are not permitted on page 1 of this document, no Intranet or Internet user is permitted to:

Retrieve, send, copy or display offensive messages or pictures.
Use obscene or racist language.
Harass, insult or attack others.
Damage computers, computer systems or computer networks.
Violate copyright laws.
Use another user's password.
Trespass in another user's folders, work or files.
Use the network for commercial purposes.

Supervising and Monitoring Usage

Teachers should guide pupils toward appropriate materials on the Intranet/Internet. This will avoid a great deal of time wasting as well as going some way towards monitoring the sites accessed by pupils.

Internet access for pupils in schools should be available only on computers that are in highly-used areas of the school such as classrooms, libraries, study rooms and ICT Suite. Machines, which are connected to the Intranet/internet, should be in full view of people circulating in the area. Primary aged pupils should never use Intranet/Internet services without close supervision. If teachers wish pupils in primary schools to surf the net, it is strongly advised that the pupils be restricted to a "walled garden site" such as yahooligans.com. There is lots of material to search through at this site, not all of it is educational, but it is all child-friendly.

While using the Internet at school, pupils should be supervised. However, when appropriate to their age and their focus of study, pupils may pursue electronic research independent of staff supervision, this should be at the discretion of the teacher in charge.

In all cases pupils should be reminded of their responsibility to use these resources in line with the school policy on Acceptable Use.

Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on the North Yorkshire LA Intranet or school servers to be absolutely private. An email is as private as a postcard, it is quite likely that no one other than the sender and receiver will ever read it, but others could if they were inclined.

Filtering External Websites

It is an absolute requirement that access to the Internet provided to staff and pupils in any school or educational institution through any Internet Service Provider (ISP) is a blocked or filtered service. Helmsley CP School Intranet uses 'Smoothwall' which is a blocking service, updated regularly. All users should be aware that the LA can and does track and record the sites visited and the searches made on the Intranet/internet by individual users.

Schools should advise parents that they provide filtered and monitored access to the Internet for pupils. However, they should also be aware that with these emerging and constantly changing technologies there is no absolute guarantee that a pupil cannot access materials that would be considered unsuitable. The chance of just coming across such materials is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search. If you are unfortunate enough to come across any offensive web pages, whilst using school equipment, you are obliged to make a note of the address and report it to your child's class teacher or headteacher who will then take the appropriate action to block the site.