Coppice School

E-Safety Policy

Date Published	
Approved Date	June 2020
Review Cycle	Annually
Review Date	June 2021

An academy within:

nexus
Multi Academy Trust

“Learning together; to be the best we can be”

E-Safety Policy

1. Overview

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Internet Use Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

Our e-Safety Policy has been written by the school, in compliance with the BECTA (British Educational Communications and Technology Agency) Guidance.

The school's e-safety policy will operate in conjunction with other policies including those for ICT, Student Behaviour, Bullying, Curriculum, Child Protection, Data Protection and Security.

The school will appoint an e-Safety Coordinator. This will be the Designated Child Protection Co-ordinator as the roles overlap.(Linda Redfern) This policy relates to the school's Internet facility. The purpose of the policy is to protect children from undesirable materials on the Internet, to protect them from undesirable contacts over the Internet and to prevent unacceptable use of the Internet by children and adults. The focus of the policy is on both personal and shared responsibility. The policy also addresses legal obligations with respect to copyright and data protection.

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.

Pupils may use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning

The school Internet access will be designed expressly 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 Internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

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.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3. Definitions

Undesirable materials

- Pornographic images or obscene text on Internet web sites
- Language that is abusive, profane, inflammatory, coercive, defamatory, blasphemous or otherwise offensive on web sites or in e-mail messages
- Racist, exploitative or illegal material or messages on web sites or in e-mail

Undesirable contacts

- E-mail messages from unknown or unverified parties who seek to establish a child's identity and/or to communicate with the child for advertising or potentially criminal purpose

Unacceptable use

- Deliberate searching for and access to undesirable materials
- Creating & transmitting e-mail messages that contain unacceptable language or content
- Creating & publishing Internet materials that contain unacceptable language & content

Adults

- School teaching staff
- Non-teaching school staff
- Governors
- Parents/Carers
- Visitors

4. Unintentional exposure of children to undesirable materials

It is the School's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials but also unintentionally when a justifiable Internet search yields unexpected results.

To prevent such occurrences the School has adopted the following position:-

(a) The use of the Doncaster LEA as an Internet Provider, offering our school protection by:

i) the filtering of sites by a grading process

ii) the filtering of sites by language content with prohibition of sites with unacceptable vocabulary

iii) the continual review and improvement of the filtering system

b) In-School protection by:

i) adult supervision of pupils' Internet activity with no searching of the Internet allowed without a suitable adult present

N.B. Filtering software is not foolproof and will be updated regularly

In the event of children being unintentionally exposed to undesirable materials the following steps will be taken.

1. Pupils should notify a teacher immediately.
2. The E-Safety Safeguarding Lead should be notified by the teacher.
3. The incident should be recorded in a central log by which the school may reliably report the frequency and nature of incidents to any appropriate party.
4. The child's parents/carer and/or the School Governors should be notified at the discretion of the Head according to the degree of seriousness of the incident.
5. Any material that the school believes is illegal must be reported to the E-Safety Safeguarding Lead who will then report to the appropriate agencies such as IWF or CEOP.

5. Intentional access of undesirable materials by children

Children must never intentionally seek offensive material on the Internet. Any transgression should be reported and recorded as outlined above. Any incident will be treated as a disciplinary matter and the parents of the children or children will normally be informed

6. Deliberate access to undesirable access by adults

Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LEA consulted.

7. Receipt and transmission of e-mails by children

It is recognised that e-mail messages received or transmitted by children can contain language or content that is unacceptable. It is also recognised that some people may try to use e-mail to identify and contact children for unacceptable reasons.

To avoid these problems the School has adopted the following practices:

a) pupils may only use approved e-mail accounts on the school system
b) allowing pupils to read e-mail messages only when an adult is present or when the messages have been previewed by the teacher
c) taking steps to verify the identity of any school or child seeking to establish regular e-mail communications with this school
d) allowing pupils to send e-mail messages only when the contents have been approved by the teacher
e) avoiding the personal identification of pupils either by never revealing the child's surname, address or other information which might identify his/her whereabouts or by using 'internet aliases' for each child
f) pupils must not arrange to meet anyone without specific permission
g) e-mails 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
h) The forwarding of chain letters is not permitted.

If staff believe that children have been targeted with e-mail messages by parties with criminal intent the messages will be retained, the incident recorded and the Governors and child's parents informed. Advice will also be taken regarding further steps.

8. Publishing of materials on the Internet

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.

It is recognised that staff and children may at some time produce and publish materials on an Internet web site associated with the School.

No materials will be published on the Internet which contain any unacceptable images, language or content. Infringement of this rule will be taken as a serious disciplinary issue.

No materials will be published on the Internet which will reveal the identity of any child.

9. Social networking and personal publishing

The school will block/filter access to social networking sites.

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 or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

School staff using social networking sites should not have any reference to the school showing on their profiles in any way; this includes uploaded photographs taken at school events, comments which refer to any school events/activities or thoughts/feelings connected to the working day, being an on-line 'friend' with a student at the school, including student parents/carers.

10. Use of the School Internet by visitors and guests

Members of school staff will take responsibility for the actions of any adult guests or visitors to whom they allow use of the school Internet facilities. The essential 'dos and don'ts' will be explained to such visitors and guests prior to their use of the Internet.

Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.

11. Responding to incidents of misuse

Minor incidents:

- copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement).
- Downloading materials or images not relevant to their education, in direct breach of the school's acceptable use policy.

11. Legal Considerations

It is recognised that all materials on the Internet are copyright unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected. Internet materials will contain due copyright acknowledgements for any third party materials contained within them.

11. Parental/carers approval

Photographs of children and materials produced by children will not be published on the Internet without parental/carers approval.

12. Managing emerging technologies and mobile technology use

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Staff will be issued with a school phone where contact with pupils is required.

12. 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. Neither the school nor Doncaster LEA can 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.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

E-Safety Safeguarding Lead *responsibilities:*

- Develop and review appropriate internet safety policies and procedures and Progression of E-Safety knowledge and skills maps.
- Development of management protocols so that any incidents in which internet safety is breached are responded to in an appropriate and consistent manner, with the appropriate authority to take action as necessary.
- Maintaining a log of all incidents relating to internet safety in school.
- Making recommendations for review of policy and technological solutions on a basis of analysis of logs and emerging trends.
- Meeting regularly with the headteacher to discuss internet safety issues and review progress.
- Updating the governing body on current internet safety issues, in conjunction with the headteacher.
- Liaising with outside agencies, which may include the LEA.
- Work with the Business Manager to provide a technical infrastructure to support internet safety practices through ensuring that appropriate and effective electronic security systems are in place, such as filtering, monitoring and firewall technology, and virus protection supported by regular and thorough monitoring of computer networks.
- Documenting the location of all internet-accessible computers within the school, including mobile and wireless equipment.
- Advising on the positioning of internet-enabled computers within the school to allow easy supervision of pupils' work, and hence discourage breaches of acceptable use policies.
- Ensuring that staff PPA room computers are secure.
- Ensuring that appropriate processes are in place for responding to the discovery of legal materials on the school's network, or the suspicion that such materials exist.
- Ensuring that appropriate processes are in place for responding to the discovery of inappropriate but legal materials on the school's network.

E-Safety Safeguarding Lead *responsibilities:*

- Leading in the creation of a staff development programme that addresses both the benefits and risks of communication technologies.
- Leading in the creation of a Progression of E-Safety knowledge and skills map for pupils, maintaining an overview of activities across the school, and supporting staff with information and resources as appropriate.
- Developing a parental awareness programme, in consultation with the Friends of Coppice association, as appropriate.

Headteacher responsibilities:

- Taking ultimate responsibility for internet safety issues within the school, while delegating day-to-day responsibility to the E-Safety Safeguarding Lead.
- Ensuring that the E-Safety Safeguarding Lead is given appropriate time, support and authority to carry out their duties effectively, also, ensuring that developments at local and partnership level are communicated..
- Supporting the E-Safety Safeguarding Lead in creating an internet safety culture within the school, including speaking to staff and students in support of the programme.
- Ensuring that the governing body is informed of the issues and the policies.
- Ensuring that appropriate funding is allocated to support internet safety activities throughout the school for both the technical infrastructure and inset training.
- Promoting internet safety across the curriculum.

Governing body responsibilities:

- Reviewing internet safety as part of the regular review of child protection and health and safety policies.
- Developing an understanding of existing school policies, systems and procedures for maintaining a safe ICT learning environment and supporting the headteacher in implementing these, including ensuring access to relevant training for all school staff.
- Supporting the headteacher in developing an appropriate strategy and plan for dealing with the media should serious incidents occur.
- Ensuring the appropriate funding is authorised for internet safety solutions, training and other activities as recommended by the headteacher, as part of the wider remit of the governing body with regard to school budgets.
- Promoting internet safety to parents, and providing updates on internet safety policies with the statutory 'security' section of the annual report.

Subject Leads/Lower/Upper School Leads responsibilities:

- Developing additional internet safety policies where necessary within the subject area/key stage – the policies should outline the importance of embedding internet safety messages within the context of the curriculum – the Progression of E-Safety knowledge and skills map.
- In consultation with the E-Safety Safeguarding Lead consider how to position departmental computers so that pupils can be suitably supervised.
- Ensuring a co-ordinated approach across the subject/school to teaching internet safety issues. This includes the responsibility of departmental staff to remind all pupils of the risks, and the pupils' responsibilities, whenever ICT is used.

Heads of Lower/Upper school responsibilities:

- Acting as a key member and first point of contact for the E-Safety Safeguarding Lead supporting them in the development and maintenance of appropriate policies and procedures relating to pupil welfare.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people.
- Ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the E-Safety Safeguarding Lead in line with school internet safety procedures.
- Ensuring that pupils who experience problems when using the internet are appropriately supported, working with the E-Safety Safeguarding Lead, and/or child protection officer as appropriate.

Classroom teachers and teaching assistant responsibilities:

- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people.
- Implementing school internet safety policies through effective classroom practice.
- Ensuring any instances of ICT misuse, whether accidental or deliberate, are dealt with through the proper channels, reporting to the E-Safety Safeguarding Lead in line with school internet safety policies.
- Ensuring that they provide the necessary support to pupils who experience problems when using the internet, working with the E-Safety Safeguarding Lead and/or child protection officer.
- Planning classroom use of the internet and ICT facilities to ensure that internet safety is not compromised; for example evaluating

websites in advance of classroom use (for example, by bookmarking and caching sites) and ensuring that the school filtering levels provide appropriate protection for themes being used.
- Embedding teaching of internet safety messages within curriculum areas wherever possible – the Progression of E-Safety knowledge and skills map.
- Maintaining an appropriate level of professional conduct in their own internet use both within and outside school.

Child Protection Officers responsibilities:

- Seeking professional development on the safety issues relating to use of the internet and related technologies, and how these relate to children and young people, refreshing this knowledge on a regular basis.
- Liaising with the E-Safety Safeguarding Lead on specific incidents of misuse, and providing follow-up counselling and support on both victims and perpetrators as appropriate.
- Taking a proactive role in the internet safety education of pupils.
- Developing systems and procedures for supporting and/or referring on pupils referred to them as a result of breaches of internet safety within schools.
- Developing systems and procedures for pupils who self-refer, and those pupils identified as suspected 'victims' by teaching staff.
- Developing relationships with colleagues at LEA level and other organisations that can provide advice, referrals or resources on issues relating to child protection on the internet.

Pupils responsibilities:

- Contribute to school internet safety and acceptable use policies through involvement in the school council.
- Upholding school policies relating to acceptable use of the internet and other communications technologies.
- Developing their own set of safe and discriminating behaviours to guide them whenever they are online.
- Reporting any incidents of ICT misuse within school to a member of the teaching staff.
- Seeking help or advice from a teacher or trusted adult if they experience problems when online, or if they receive any content or contact which makes them feel uncomfortable in any way.
- Communicating with their parents and carers about internet safety issues, and upholding any rules for safe internet use in the home.

13. 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 Head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Parents/carers and pupils will need to work in partnership with staff to resolve issues.

14. Review of this policy

This policy will be reviewed regularly.

Managing Internet Access in the Classroom

Notes for Teachers

1. The Internet should be seen as an extension of the school library which facilitates resource sharing, communication and innovation.
2. The issues of responsibility that arise from use of the Internet should be addressed before access is given.
3. All users should be aware of and adhere to an agreed code of practice.
4. Pupil access should always be supervised and monitors placed where the screen can be viewed from a distance.
5. Teachers should consider checking pupils' Internet searches and using history pages to monitor access.
6. Teachers should consider selecting web sites as part of their lesson planning in order to guide children's searches.
7. Contributions to web pages should be original work and should be checked for accuracy before being submitted.

Guidelines for Students and Staff

Using the Computer

1. Make sure you have permission to use the computer.
2. Use your own log in and password.
3. Save your work regularly.
4. Ask an adult to help you if there is a problem with the computer.
5. Close all programmes when you have finished and leave the computer ready for someone else to use.
6. Use the computers with care. They are there for everyone to use.

Internet and E-mail

1. Narrow down Internet searches as much as possible before you start.
2. Use 'Bookmarks' and 'Favourites' to save interesting sites.
3. Ask before you print anything and note the source.
4. Do not give personal information about yourself (e g name, address or location) to anyone.
5. Tell an adult if you come across anything that makes you feel uncomfortable.

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

e-Safety Rules

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

e-Safety Rules

These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Coppice School

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	***Form:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's/Carers Consent for Web Publication of Work and Photographs

I agree that my childs' work may be electronically published. I also agree that appropriate images and video that include them may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's/Carers Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

I agree that I will not accept any on-line 'friend' requests or send on-line 'friend' requests from/to members of school staff.

Signed:	***Date:***

Please print name:

Please complete, sign and return to the school office