E-Safety Policy and Acceptable Use Agreements

Approved by: **Full Governing Body**

Date of Approval **September 2024**

E-Safety in school is overseen by the head teacher and supported by the Computing Subject lead. This policy should be read in conjunction with the Safeguarding & Child Protection Policy and the Information (Data Protection) Policy.

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. It has become part of everyday life in education, business and social interaction. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning. Similarly, at home, many children have access to a range of technologies and it is part of the responsibility of school, alongside parents, to help to educate children in how to stay safe.

Who does the policy apply to?

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Overall aim

Our overall aim is that all children at Fishergate will understand how to use the internet effectively and how to stay safe when accessing the internet, both at school and at home.

Objectives

All children at Fishergate should learn:

- that the internet contains an almost infinite amount of information which, when used appropriately, can be educational and entertaining.
- that most of the information on the internet is not verified and therefore has to be checked for accuracy.
- that there is some content on the internet which is inappropriate or even illegal and should be avoided.
- that the internet is a powerful tool for communication which allows us to be in instant contact with people from all over the world.
- that some people misuse the internet to communicate unkind or hateful messages (including cyber bullying) and that these people should be reported.
- that some people on the internet are not who they say they are.
- that a small number of people want to hurt children and could use the internet to make contact with them.
- how (or who) to report content or messages that are inappropriate, harmful or upsetting.
- that harmful and upsetting behaviour online may affect their mental health and they should know who to speak to if this is the case if they experience this.

Through computing and subject lessons, pupils will develop an understanding of the uses, importance and limitations of finding information on the internet.

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate the information they find on the internet.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to using the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Through computing and subject lessons, pupils will develop an understanding of how to use the internet to communicate safely and appropriately.

- Pupils will be taught how to use email effectively, including checking for bogus messages.
- Older pupils will be taught how to share information using collaborative tools, including Google Workspace, and how to comment on other people's posts appropriately.
- Pupils will be taught how to respond to inappropriate comments (cyber bullying). Who to speak to or contact if they experience this.
- Pupils will be taught not to share passwords or personal information.
- Pupils will be taught how to respond to unsolicited attention.

Methodology

In line with all City of York schools, there is a 'firewall' preventing harmful material and inappropriate sites from being accessed at school. This is a comprehensive filtering platform using dynamic and group based filtering including new requirements around child safety and anti-radicalisation. It is designed to protect schools from inappropriate on-line content, as well as meeting or exceeding the current and recommended safeguarding children legislation. Detailed alerts and reporting are configured to alert the Authority help-desk of an incident at school, enabling a fast response to ensure children's safety. City of York council are responsible for updating and maintaining this. Children should not have any unsupervised internet access in school, and should never be given access to the internet under a staff member's login or on staff iPads etc. Even with all of the above in place no system is infallible. Therefore children are encouraged to talk to a member of staff if they see something on the internet which makes them feel uncomfortable. If unsuitable content were accessed, the staff have responsibility to report it to the Computing subject lead and the head teacher.

E-Safety is part of the National Curriculum for Computing. It is explicitly taught in all year groups as part of Fishergate's Computing curriculum.

To complement our teaching, we use resources from:

- Purple Mash, Espresso Coding and Scratch – online software programs.
- www.childnet.com (Adventures of Kara, Winston and the SMART crew) (Smartie the Penguin) (Digiduck's Big Decision)
- https://www.thinkuknow.co.uk/ CEOP Education – e-safety
- https://www.bbc.com/ownit

- www.digizen.org (Useful information for parents and teachers)
- https://nationalonlinesafety.com/ (Useful information for parents and teachers)
- https://studio.code.org coding and e-safety

Children, staff and visitors are all made aware of our 'Safe Use of the Internet Guidelines'. (See appendix at the end of this policy). Guidelines are on classroom walls, in the school office and published on the School Website.

In class, staff model good internet practices and etiquette.

In addition:

- The Computing lead will run a parent/carer workshop covering e-safety and the computing curriculum.
- An e-safety update is regularly included in the school's newsletter.
- Useful tips/information are regularly updated on the school's website.

Mobile Phones and other handheld technology

Pupils are not permitted to have smart phones or smart watches in school. If parents and carers feel their child needs to be able to contact them, for example if they are in Year 5/6 and walk to and/or from school independently, pupils may bring a 'dumb' phone, which enables them to text or call, but not to access the internet.

Reporting

All incidents or disclosures will be treated with the utmost care and diligence. Children making disclosures will be given the opportunity to say what they need in a safe space, with no leading questions. However, they will also be told that a member of staff cannot keep their disclosure secret and will have to inform another member of staff. All disclosures should be recorded on CPOMS and brought to the Phase Leader and Head Teacher's attention. The school's safeguarding policy will then be followed.

- Apparent or actual misuse or illegal activity could include:
- child sexual abuse images
- 'sexting'
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- inappropriate messages or online bullying (mobile phones, social media, email etc)
- other criminal conduct, activity or materials e.g county lines evidence/ FGM etc

Fishergate's
Safe Use of the Internet Guidelines
EYFS & Key Stage 1

Using Computers and the Internet

Follow these simple rules in school to keep safe and be fair to others.

- I will be careful with the computers, including making sure my hands are clean before use of equipment.

- I will use the computers only for school tasks and homework.

- I will not send messages to anyone, unless my teacher says it is OK.

- I will never give out my name, home address, telephone number, or any other information about myself or my family.

- I will tell my teacher if I find any words or pictures which make me feel unhappy or confused.

Fishergate Primary School
Safe Use of the Internet Guidelines
Key Stage 2

Using Computers and the Internet

At Fishergate, we think that computers are a fantastic aid to learning.

The internet opens up wonderful possibilities for finding out about anything that interests us. It is up to all of us to make sure we use it wisely.

Follow these simple rules to keep safe and be fair to others.

- I will take good care of all the computer equipment and treat it with respect, including making sure my hands are clean before use of equipment.
- I will use the computers only for school tasks and homework.
- I will check with the teacher before I use my own USB stick / DVD / memory card.
- I will not send or receive messages or emails to or from anyone, unless I have the teacher's permission.
- Any messages I do send will always be polite and respectful.
- I will never give out my surname, home address, telephone number, or any other information about myself or my family.
- I will let a teacher know if I find any pictures or writing which make me feel uncomfortable. I know I will not be in trouble for this.
- I will keep my own passwords private and not ask anyone for their password.

Safe Use of the Internet Guidelines

All Staff and Visitors

All adults working with ICT equipment in Fishergate School must ensure that they have read and agree to abide by the following rules.

For personal use:

- Keep the school passwords private within school.
- Never use unencrypted memory sticks to transfer any information about pupils.
- Use the school email system, for any messages about pupils or staff – never a personal email account.
- Ensure all messages sent via the internet are polite and professional.
- Do not store any information about individual children on your computer at home.
- Ensure that home computers have virus checking software so there is no risk of transferring viruses from USB memory sticks.
- Do not open other people's files without their permission.
- Do not release personal details including phone numbers, addresses or personal email addresses of any colleague or pupil.
- Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.
- Do not attempt to visit sites which might be considered inappropriate in a primary school. All sites visited leave evidence on the computer.
- Use of school Internet access for business, profit, advertising, personal shopping or political purposes is strictly forbidden.

When using the Internet with children

- Repeatedly remind children of the rules for safe use of the internet.
- Watch for accidental access to inappropriate materials and report the offending site to the Computing Leading Teacher.
- Ensure children are appropriately monitored when using the internet.
- Ensure you are aware of the children in your class whose photographs may not appear on the website or social media.
- Ensure photographs of children are not named.

Stay safe online all of the time!

Don't give out personal information

Keep your personal information private and use it on safe sites only.

Keep your passwords safe

Make sure you don't share your password with others and always log out of a device or app when you have finished.

Tell a trusted adult

If you have a problem or see something you don't like, tell a parent, carer or trusted adult and they will help.

Report and contact help

If you feel unsafe or unhappy press the REPORT button. If you can't or don't want to talk to a trusted adult, contact the NSPCC or Childline for help.

https://www.childline.org.uk/get-support/contacting-childline/

ChildLine 0800 1111

NSPCC

CLICK CEOP Internet Safety