St Helens Primary School

e-Safety Policy

Reviewed by: FGB

On: December 2022

Next review due: December 2023

Chair of Governors: Gary Booth

Signature: *Gary Booth*

ST HELENS PRIMARY SCHOOL

E-SAFETY POLICY

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.

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.
- 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.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Managing Internet Access

Information system security

- The school's ICT system's capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school's system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail 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.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the website should be the school's address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The ICT manager in conjunction with the Head teacher take editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified without parental consent
- Pupils' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Social Media
  WhatsApp have just announced a change to their terms and conditions for users based in Europe. Users will now need to be 16 to use WhatsApp.

  Nearly all other social media services require users to be at least 13 years of age to access and use their services. This includes Facebook, Snapchat, Twitter, Instagram, Musical.ly and Skype.

  Whilst there is no age restriction for watching videos on YouTube, users need to be 13 or older to have their own YouTube account (enabling them to subscribe to other channels, like videos, post comments, share their own content and flag inappropriate content).

Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Head teacher.
- 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 the schools is allowed.
- Mobile phones will not be used during lessons or formal school time. Mobile phones are stored in the office during the day.

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 ‘Acceptable ICT Use Agreement’ before using any school ICT resource. See Appendix 1.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.
- Access to the Internet will be supervised by teaching staff.
- Parents will be asked to sign and return a consent form.

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. The school cannot 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.
- Independent e-safety training is undertaken every three years.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Head teacher.
- 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.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School's e-Safety Policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School's e-Safety Policy by newsletter and website.
- Parents are encouraged to monitor pupil's Internet use and follow guidance regarding the use of social media.

The e-Safety Policy and its implementation will be reviewed annually.

This policy links to the following policies:

- Child Protection Policy
- Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Drug Policy
- Complaints Policy

Appendix 1: Acceptable use agreement (pupils and parents/carers)

<table>
<tr><th colspan="2">Acceptable use of the school's ICT systems and Internet: agreement for pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of Pupil:</td></tr>
<tr><td colspan="2">
When using the school's ICT systems and accessing the Internet in school, I will not:

Use them for a non-educational purpose.
Use them without a teacher being present, or without a teacher's permission
Access any inappropriate websites.
Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity).
Use chat rooms.
Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
Use any inappropriate language when communicating online, including in emails.
Share my password with others or log in to the school's network using someone else's details.
Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer.
Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

If I bring a personal mobile phone or other personal electronic device into school:

I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission.
I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.

I agree that the school will monitor the websites I visit.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the school's ICT systems and internet responsibly.
</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement:
I agree that my child can use the school's ICT systems and Internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer)</td><td>Date:</td></tr>
</table>

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the Internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, **I** will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. **I** agree that the school will monitor the websites **I** visit. I will take all reasonable steps to ensure that work devices are *secure* and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. **I** will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**