NEWBOLD SCHOOL
E-Safety ICT Policy (online safety)

Updated September 2024 by Mrs Crissey & Mrs Jennings
Ratified by Newbold Board of Governors : November 2024
Next review: Autumn Term 2025

This E-Safety Policy relates to other policies, including those for ICT, bullying and for child protection.

- The school's E-Safety coordinator, is Mrs Chaudhri
- Issues of suspected inappropriate use by pupils or teachers are flagged up by our Smoothwall system and reported to the Designated Safeguarding Lead (DSL).
- The E-Safety Policy and its implementation will be reviewed annually.

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 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.
- The internet is helpful for homework (using Seesaw, for example) to help reduce the use of handling paper to help us protect our environment.

Internet use will enhance learning

- The school internet access includes a filtering system to ensure that only sites appropriate to the age of pupils can be used in school. All instances of inappropriate use will go to the safeguarding Designated Lead Officer to be checked.
- Teachers will be able to monitor the sites each pupil is using during lessons and pupils know that this is the case.
- Pupils will be taught about acceptable internet use and what is not acceptable; they will be given clear and appropriate 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 the difference between causal responses to their friends (e.g. on social media and texts) and more formal responses to their teachers.
- Seesaw is not open to external users and children's work is not open for other children to view without permission.

Pupils will be taught how to evaluate internet content

- Staff should 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.

Managing Internet Access

Information system security

- The ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed, and updated regularly.
- Filtering and monitoring is managed by Smoothwall.

E-mail

- Pupils may only use the approved school email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil e-mail communication must only take place via a school email address or from within the learning platform that is monitored.
- E-mails sent to an external organisation should be written carefully and checked 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 web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the web site or in blogs, or forums, particularly in association with photographs.
- Written permission from parents, guardians or carers will be obtained at the beginning of each academic year before photographs of pupils are published on the school website and/or Seesaw.

Managing filtering and monitoring

In line with KCSIE (2023), we have an increased responsibility regarding the school's filtering and monitoring systems for IT.

- All staff and Governors understand their expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- All staff and governors have read and understood the published DfE guidance on filtering and monitoring. https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

- filtering and monitoring provision will be reviewed at least annually
- harmful and inappropriate content is blocked without unreasonably impacting teaching and learning
- effective monitoring strategies are in place that meet our safeguarding needs and KCSIE 2023 requirements.
- roles and responsibilities for staff and Governors have been identified and assigned to manage filtering and monitoring systems.

  Mrs Chaudhri is our E-Safety Officer.

  Mrs Illingworth is responsible for the IT curriculum.

  The DSL (Head Teacher) takes lead responsibility.

- The school will closely work with our technicians to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Officer or Head Teacher who will arrange with the technician to filter the site.

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.

Mobile Phones

- Staff are not permitted to use mobile phones during lessons or formal school time, unless there is an emergency and it is the only way to summon help. They should not use their mobile phones in the presence of children, take photos of children or engage in any form of mobile phone communication with children, including sharing of photos.
- Mobile phones will be stored away during lesson times
- Any exceptions will be reported to the DSL/DDSL or office staff (to use for music purposes linked to our sound system for PE, music, sports day, assemblies etc).

- Pupils are not permitted to carry mobile phones in school. Any child who is given a mobile phone as a necessary means of contact with parents (e.g. for walking home alone) must leave it in the school office in the morning and pick it up only when they are leaving to go home.
- All electronic devices with imaging and sharing capabilities (ie. Smart watches which have a camera device installed) are not permitted for use during the school day for neither staff nor pupils.
- Sending abusive or inappropriate text messages is forbidden for both staff and pupils.
- Sexting is forbidden. Any member of staff caught sending messages with sexual content to any child under the age of 18 will be reported to the police.

Social Media:

- Staff are not permitted to accept friend requests from any pupil at Newbold School or converse with them on social media at any time, either on or off site.
- Staff are expected to keep their social media accounts private.
- Staff are not permitted to post inappropriate language, photos or videos that could bring the reputation of the school into question (e.g. use of offensive language, posting crude/lewd or drunken photos).
- Children are not allowed to access social media sites (e.g. Facebook) during school hours.

Use of Seesaw

- Children are not allowed to engage in casual chat on Seesaw. This platform will be used only for work or receiving help from teachers. It is not designed for social interaction.
- Children's work will not be shared with other children on Seesaw unless the teacher wishes to use good work as an example to others.
- Children will not be able to view and make comments on other children's work, unless during a peer evaluation exercise mediated by the teacher. Guidance on appropriate comments will be provided.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations..

Policy Decisions

Assessing risks

- The school will use a filtering system to prevent access to inappropriate material.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

e-safety complaints

- Complaints of internet misuse will be received by the e-safety officer, who will take it to the headteacher.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school child safety procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer if there is a need to establish procedures for handling illegal issues.

Community use of the internet

All use of the school internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Communications Policy

Introducing the e-safety policy to pupils

- e-safety rules will be posted in KS1 and KS2 classrooms
- Pupils will be informed that network and internet use will be monitored and that teachers can see what they are viewing or doing online through the central network system.
- Pupils at Key Stage 2 will be made aware of e-safety issues and possible misuse through PSHE curriculum.

Staff and the e-Safety policy

- All staff will be given the school's E-Safety Policy and its importance will be explained in their safeguarding training.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be made aware of procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school's e-Safety through publication on the school's website
- Parents and carers will from time to time be provided with additional information on e-safety as necessary.