MOTTRAM ST. ANDREW PRIMARY ACADEMY

e-safety POLICY

e-safety encompasses the use of personal devices, new technologies, internet and electronic communications. It highlights the need to educate pupils about the benefits and risks of using technology and social networking websites and applications and provides safeguards and awareness for users to enable them to control their on line experience.

This e-safety Policy has been written by the school, building on the Cheshire e-safety Policy and government guidance.

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

The e-safety Policy relates to the Teaching and Learning Policy, Behaviour Policy, the school Safeguarding policy, Staff Code of Conduct for ICT and Pupil e-safety Rules.

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 use will be designed expressively for pupil use and will include filtering appropriate to the age of the pupils.

Pupils and families 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.

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.

Online safety:

The e-safety leader and ICT Leader have undertaken Child exploitation and On-line Protection (CEOP) training and lead the teaching of e-safety in all year groups.
Designated upper KS2 pupils have attended CEOP training and organise events for the children to highlight the importance of staying safe online.

The school's website has a CEOP reporting button.

Social networking and personal publishing:

- The school has access to social networking sites.
- Pupils will be told 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 some social network spaces outside school is inappropriate for primary aged pupils.

Managing Internet Access

Information System security:

School ICT systems and security will be reviewed regularly.

Virus protection will be installed on every computer and will be set to update automatically.

Staff e-mail:

- Staff must report any offensive emails to a member of the leadership team.
- E-mail sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper.
- The forwarding of chains is not permitted.

Published content and the school Website:

The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Head Teacher will take overall 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.

Pupils' full names will not be used anywhere on the website or social media, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published by the school.

Managing Filtering:

The school will work with the LA, and our technical support 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 e-safety leader.

Managing Videoconferencing:
Videoconferencing will be appropriately supervised, by the class teacher, for the pupils' age.

Managing personal devices and emerging technologies:
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school if necessary.

Pupil's personal devices are not normally allowed in school. In exceptional circumstances pupil devices may be stored in the school office and returned to them at the end of the day.

The taking of photographs of pupils on staff personal devices is prohibited.

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 'Staff Code of Conduct for ICT' before using any school ICT resource.

All students and parents must read and agree to the 'Pupils' Safety Rules'.

Within the Primary School access to the Internet will be supervised. Lower down the school there will be access to specific, approved on-line materials.

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 regularly audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints:
Complaints of Internet misuse will be dealt with by the e-safety Leader.

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 the school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

Community use of the Internet:
The school will liaise with local schools to establish a common approach to e-safety.

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 e-safety policy and its importance 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 e-safety Policy in newsletters and on the school website.
- Parents will be required to sign the e-safety agreement and will be expected to attend an e-safety evening at the school.

Related Policies
Teaching and Learning; Behaviour, Safeguarding; Staff Code of Conduct for ICT, ICT Policy; e-safety rules.

E-safety leader: Mrs H Woolley
ICT leader: Mrs K Cavanagh