MOTTRAM ST. ANDREW PRIMARY ACADEMY

E-SAFETY POLICY

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

Teaching and Learning

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 will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

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 attend CEOP training and organise events for the children to highlight the importance of staying safe online.

The school internet will include filtering appropriate to the age of the pupils.

Pupils will be taught what internet use is and is not acceptable.

Social networking and personal publishing:

- The school has access to social networking sites.
- Pupils will be told never to give out personal details 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.

Information sytem 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 email:
Staff must report any offensive emails to a member of the leadership team.

Email 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.

Publishing pupil's images and work:
Photographs that include pupils will be selected carefully.

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.

Below are some things staff have been told to consider when delivering virtual lessons, especially where webcams are involved:

- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and staff will ensure that the background behind them does not contain anything too personal.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms specified by senior managers to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held and overview of content.

In addition, staff supporting remote learning have been told that they must record whether any safeguarding issues were noted. If concerns were reported/observed staff will record the detail of this and the date/time these were shared with the DSL as per normal safeguarding reporting processes.

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 certain circumstances pupil devices may be stored in the school office or in a locked drawer in the classroom 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 GDPR 2018.

Policy Decisions

Authorising Internet access:
All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

Pupils' Safety Rules are shared with all pupils.

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 Headteacher.

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

Parents complaints will be dealt with using the complaints procedure.

Communications

Introducing the E-Safety Policy to pupils:

- E-safety rules will be regularly discussed with the pupils.
- Pupils will be informed that network and internet use will be monitored.

Staff and the E-Safety Policy:

- The E-safety Policy is shared with all staff.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

Enlisting parents' support:

- E-safety information is shared with parents to support them in keeping their children safe online at home.