MOTTRAM ST. ANDREW PRIMARY ACADEMY

ONLINE SAFETY POLICY

Using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Online 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.

Online Safety

Online safety is a key component of our Computing Curriculum

The Computing Lead has undertaken Child Exploitation and On-line Protection (CEOP) training and ensures that online safety is taught in all year groups.

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.

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 our technical support provider to ensure systems to protect pupils are reviewed and improved.

Smoothwall is used to filter content, monitor online activities, and provide comprehensive reporting. The headteacher receives daily reports directly.

If staff or pupils discover an unsuitable site, it must be reported to the Computing Lead, Headteacher or Deputy Headteacher.

Managing Virtual Lessons:
Virtual lessons 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, for example, mobile phones, 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.

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.

Handling online safety complaints:

Complaints of internet misuse by a child will initially be dealt with by the class teacher and escalated as appropriate within our behaviour policy.

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

Any complaint about staff misuse must be referred to the Headteacher.

Parents complaints will be dealt with using the complaints procedure.

Communications

Pupils:

- How to keep safe online is part of our Computing Curriculum and is regularly discussed with the pupils.
- Pupils will be informed that network and internet use will be monitored.

Staff:

- The Online Safety Policy is shared with all staff.
- Staff are made aware that internet traffic can be monitored and traced to the individual user.

Parents:

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