MEADOWPARK School

E- SAFETY POLICY

Date: May 2021

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms (MLE) and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

At Meadowpark School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher has ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named technical e-Safety Lead in our school is the Bursar. The named staff member for responsibility for day to day Online Safety issues is the ICT coordinator Mrs Beaumont who allocates passwords and ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.

Writing and reviewing the e-Safety policy

This policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following school policies: Child Protection, and Curriculum

E-Safety skills development for staff

- All members of staff receive information and training on e-Safety issues through the coordinator at staff meetings.
- All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what todo in the event of misuse of technology by any member of the school community.
- All new members of staff receive information on the school's acceptable usage. This is outlined in the staff code of conduct.

- All members of staff incorporate e-Safety activities and awareness throughout the computing curriculum.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teache-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help ifthey experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline.
- 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.

Managing Internet Access

Information system security

- Internet Access is filtered for all users using 'Clean Browsing'

E-mail

- Pupils may only use approved school e-mail accounts on the school system when supervised in lessons.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- email sent to an external organisation should be written carefully and authorisedbefore sending, in the same way as a letter written on school headed paper.

Published content and the school web site

The contact details on the school website are the school address, e-mail and telephone number. Staff or pupils' personal information is not published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period

that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and will not enableindividual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the school website, particularly inassociation with photographs.
- Pupils' work can only be published by outside agencies with the permission of thepupil and parents.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites and social media e.g. School performances and assemblies etc.

Social networking and personal publishing

- Pupils and parents will be advised that the use of social network spaces outsideschool is inappropriate and or illegal (e.g. Facebook) for primary aged pupils.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff should not accept friend requests from parents if they use thesesites, so that relationships remain professional at all times.

Managing filtering

- Uses the filtering system 'Clean Browsing' which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account

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.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Anyphones that are brought to school are sent to the school office and kept thereuntil the end of the day.
- The sending of abusive or inappropriate text messages or emails outside school isforbidden.
- Staff will use a school phone where contact with parents is required.

Protecting personal data

The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond theschool/|
The school will hold personal information on its systems for as long as individualmembers of staff remain at the school and remove it in the event of staff leaving or until it is no longer

required for the legitimate function of the school.We will ensure that all personal information supplied is held securely, in accordance with our data privacy policy Each teacher has the right to view personal information that the school holdsand to have any inaccuracies corrected.

Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access
- Access to the Internet will be by directly supervised and to specific, approved on-line materials.

Password Security

- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. The school will 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 Headteacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints and concerns of a child protection nature must be dealt with in accordance with school child protection procedures. For example evidence of: inappropriate online relationships; a child watching pornography or any '18' films on a regular basis; online/digital bullying, harassment or inappropriate image sharing etc.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-Safety policy to pupils

- E-Safety rules are displayed in the ICT suite and discussed regularly with the pupils. All staff are aware that e-safety content must be taught each term and at relevant points throughout e.g. during PSHE lessons//anti-bullying week/Safer Internet Day.
- Pupils will be informed that network and Internet use will be monitored.
- The school is vigilant when conducting 'raw' image search with pupils e.g. Google image search

Staff and the e-Safety policy.

- Any information downloaded must be respectful of copyright, property rights and

privacy.

- All members of staff are aware that internet traffic can be monitored and tracedto the individual user. Discretion and professional conduct is essential.

<u>Parents</u> and the e-safety policy

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.

This policy was approved on 11th May by the Headteacher and will be reviewed annually.