E- SAFETY POLICY

Review Date	**September 2023**
Reviewed By	Danielle Clowes & Diane Laing
Next Review	**September 2024**
Summary of Changes	First Edition

Approved by:

Head Teacher: **Date: 06/09/2023**

Deputy Head Teacher: **Date:06/09/23**

DSL: **Date:06/09/2023**

CONTENTS

1. Purpose - 2 -
2. Introduction - 2 -
3. Roles and Responsibilities - 3 -
4. Teaching and Learning - 4 -
5. Managing Internet Access - 5 -
6. Policy Decisions - 6 -
7. Communication - 7 -

1. PURPOSE

This policy is a statement of the aims, principles, strategies and procedures for e-safety throughout Emerge School. The policy provides the framework to nurture a safe digital community. 'Information Governance' refers to and encompasses the policies, procedures, processes and controls implemented to manage information. These support the school's immediate and future regulatory, legal, risk and operational requirements. Emerge is committed to ensuring all children 'Learn and Achieve' in a safe learning environment.

2. INTRODUCTION

The Internet is now regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and touch screen tablet devices. 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

Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill. Young people have access to the Internet from many

places - home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe.

At Emerge 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.

3. ROLES AND RESPONSIBILITIES

Senior Management

As e-Safety is an important aspect of strategic leadership within the school, the overall responsibility for e-safety of the school community rests with the SLT. The Head Teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be shared across the Senior Leadership Team. It is the role of SLT to keep abreast of current issues and guidance through organisations such as CEOP and 'Think U Know'.

• The Head Teacher and at least one other member of the SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

• The Head Teacher is responsible for ensuring that SLT and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues.

• The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.

• The Head Teacher will provide opportunities for parents, carers and members of the wider community to gain information and understanding about e-safety.

The role of SLT is to:

- Lead the e-safety committee.
- Take day-to-day responsibility for e-safety issues as well as reviewing the school e-safety policies and existing e-safety provision.
- Ensure all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff.
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.

Technical Staff –

The role of the technical staff will include:

• Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack.

• Ensuring that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.

• Ensuring that users may only access the networks and devices through a properly enforced password protection policy.

• Making sure they have an up to date awareness of e-safety matters and of the current e-safety policy and practices.

• Ensuring that they report any suspected misuse or problem to the Head Teacher/SLT for investigation / action / sanction.

Teaching and Support Staff -
The role of teaching and support staff will include:
• Having an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

• Reporting any suspected misuse or problem to the Head Teacher / SLT for investigation / action / sanction.

• All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.

• E-safety issues are embedded in all aspects of the curriculum and other activities.

• Students / pupils understand and to follow the e-safety and acceptable use policies.

• Monitoring the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

• In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

• National online safety day – we teach e-safety at least half termly and we participate in e-safety day.

4. TEACHING AND LEARNING

Teaching and Learning Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-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 eSafety 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 if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- 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.

5. MANAGING INTERNET ACCESS

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Appropriate anti-Virus protection is updated regularly.
- System security is overseen by our technicians
-

Email

- Pupils may only use approved email accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before 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 head teacher 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 enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Pupils' work can only be published by outside agencies with the permission of the pupil and parents/ carers.

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, e.g. School performances and assemblies etc.

Social networking and personal publishing

- The school blocks access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook) for primary aged pupils.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children, or parents as 'friends' if they use these sites.

Managing filtering

- Has the educational filtered secure broadband connectivity and so connects to the 'private' National Education Network
- The school will ensure that suitable filtering systems are in place on ICT equipment to prevent children accessing inappropriate material, in accordance with 'Keeping

Children Safe In Education 2022' (SAPHOS). The school will, however, ensure that the use of filtering and monitoring systems does not cause "over blocking", which may lead to unreasonable restrictions as to what pupils can be taught online.

- Staff will be aware of the filtering systems in place and will know how to escalate concerns where they are identified.

- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students
- Ensures network healthy through use of anti-virus software etc and network set-up so staff and pupils cannot download executable files
- Uses individual, audited log-ins for all users
- Uses EGRESS secure portal for safeguarding confidential information via email
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform
- Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils
- Provides staff with an email account for their professional use
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies

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. Any phones that are brought to school are sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages or emails outside school is forbidden.
- Staff will use a school phone where contact with pupils 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 the school/Local Authority. The school will hold personal information on its systems for as long as individual members 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 the Data Protection Act 1998. Each teacher has the right to view personal information that the school holds and to have any inaccuracies corrected.

6. POLICY DECISIONS

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement (AUA) for pupils and abide by the school's e-Safety guidelines.
- Access to the Internet will be by directly supervised and to specific, approved on-line materials.
- All staff using a school laptop will be made aware of the schools Laptop Use Policy

Password Security

- Adult users are provided with an individual network username, password and email address, which they are encouraged to change periodically.
- Key Stage Two pupils are provided with an individual username and password.
- All members of staff are aware of the dangers inherent in leaving the SIMs system, for pupil-tracking and digital registers, open and of the importance of keeping passwords secret
- All members of staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

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 a senior member of staff and reported to the e-Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by a member of SLT.
- Any complaint about staff misuse must be referred to the Head Teacher.
- 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.

7. COMMUNICATION

Introducing the e-Safety policy to pupils

- E-Safety rules are displayed in the classroom and discussed with the pupils at the start of each term. All staff are aware that at least one dedicated e-safety lesson 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 or Lycos image search
- Pupils are required to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme

Staff and the e-Safety policy

- All staff must sign the Staff Acceptable Usage Policy and a copy is kept on file.
- 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 traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
-

Parents/ Carers and the e-safety policy

- All parents/ carers, when their child joins the school, will be asked to sign the AUA for pupils giving consent for their child to use the Internet in school by following the school's e-Safety guidelines and within the constraints detailed in the school's eSafety policy, supported by the KCSIE 2022
- 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.
- Parents are encouraged to look at the school's e-safety policy and the pupil 'Acceptable User Agreement'

PUPIL ACCEPTABLE USE POLICY AGREEMENT

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet, tablet devices and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

This is how we stay safe when we use the computers:

- I will ask a teacher or an adult if I want to use the computers.
- I will use child friendly search engines when using the computers to search for websites, unless my teacher has already approved that site.
- When logging into a computer, I will use my own login and password, which I will keep secret. I will change this every term.
- I will only use activities that a teacher or an adult has told or allowed me to use. I will not use internet chat.
- When communicating online, I will not give out my home address, phone number, or arrange to meet anyone. I will only engage with people I know, or my teacher has approved and my messages will be polite and sensible.
- If I see anything that I am unhappy with or I receive messages I do not like, I will turn off the screen and tell a teacher immediately.
- I know that the school will check my computer files and may monitor the internet sites I visit.

- I will take care of the equipment and use it respectfully. I understand that if I cause deliberate damage to any electronic devices then I will have to pay reparations as part of my consequence.

- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.

Pupil/ Class: …… Date: …….