eSafety Policy

Reviewed and approved by:	Governing Body	
Date Adopted:	November 2024	
Date for next Review:	November 2025	
Signed by Name Printed:	Chair of Governors Kirsty Bull	Headteacher Jo Hall
Signed:	Kirsty Bull	Jo Hall
Date:	November 2024	November 2024

Introduction

This policy has been prepared by the eSafety coordinator and has been agreed by the eSafety group which includes the Headteacher, Governing Body, pupils, parents and members of the local community.

Our aims are to ensure that all pupils:

· will use the internet and other digital technologies to support, extend and enhance their learning;

· will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;

· will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;

· will use technologies safely.

In order to achieve these goals:

● Pupil's access to content will be subject to age-appropriate filters.

The school's filtering and monitoring system, Smoothwall, will be used to check on any breaches and these will be immediately followed up. Children are told that this is in place.

● Pupils will be taught how to effectively use the internet for research purposes.

● Pupils will be taught to evaluate information on the internet.

● Pupils will be taught to recognise online dangers and how to avoid them.

● Pupils will be taught how to report inappropriate web content.

● Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies including email.

● Pupils and staff will be provided with individual email accounts. All emails are filtered, stored and monitored. Children's email accounts are limited to communication within the school's domain.

● Pupils are not permitted to use mobile phones or smart watches on the school premises. Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (Education and Inspections Act 2006, Sections 90, 91 and 94).

Web Filtering

● The school will work with the Local Authority to ensure that appropriate filtering is in place, using the Local Authority's managed Smoothwall service. In addition, the school will manage filtering both on and off the premises using Google filtering services.

eSafety Complaints

● Instances of pupil internet / IT misuse must be reported to a member of staff.
● Staff are trained to deal with eSafety incidents. They must refer the matter to a senior member of staff who will log the incident.
● Instances of staff internet misuse should be reported to, and will be dealt with by, the Headteacher.
● Pupils and parents will be informed of the consequences of internet / IT misuse.

Whole School Responsibilities for Internet Safety

Headteacher
● Ensure that the eSafety coordinator is given appropriate time, support and authority to carry out their duties effectively.
● Ensure that the Governing Body is informed of eSafety issues and policies.
● Ensure that appropriate funding is allocated to support eSafety activities throughout the school.

eSafety coordinator (as part of a wider Child Protection team)
● Establish and maintain a schoolwide eSafety programme (inc. eSafety sessions as part of Computing curriculum, eSafety sessions as part of PSHE curriculum, eSafety assemblies, Curriculum days and supporting events such as Safer Internet Day).
● Form a school eSafety group to review and advise on eSafety policies and procedures.
● Respond to eSafety policy breaches in an appropriate and consistent manner.
● Form a school eSafety management group to review the effectiveness and impact of the policy.
● Ensure staff are informed and feel confident to deliver eSafety sessions.
● Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body
● Appoint an eSafety Governor who will ensure that eSafety is included as part of the regular review of child protection, safeguarding and health and safety policies.

● Support the Headteacher and/or designated eSafety coordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
● Ensure that appropriate funding is authorised for eSafety solutions, training and other activities as recommended by the Headteacher and/or designated eSafety coordinator (as part of the wider remit of the Governing Body with regards to school budgets).

Teaching and Support Staff
● Contribute to the development of eSafety policies.
● Adhere to acceptable use policies.
● Take responsibility for the security of data, ensuring they do not allow computers / browsers to 'remember' passwords which give access to school data / information.
● Develop an awareness of eSafety issues, and how they relate to pupils in their care.
● Model good practice in using new and emerging technologies.
● Include eSafety regularly in the curriculum.
● Deal with eSafety issues they become aware of and know when and how to escalate incidents.
● Maintain a professional level of conduct in their personal use of technology, both within and outside school, including the use of social media (staff must not make any comment on school related issues via social media. See Staff Code of Conduct.)
● Take responsibility for their professional development in this area.

Parents and Carers
● Contribute to the development of eSafety policies.
● Read acceptable use policies and encourage their children to adhere to them.
● Discuss eSafety issues with their children, support the school in its eSafety approaches and reinforce appropriate behaviours at home.
● Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
● Liaise with the school if they suspect, or have identified, that their child is conducting unsafe behaviour online.