Ellwood Community Primary School

E-Safety

E-Safety/Online Safety Policy

Introduction
E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to safely control their online experiences.

The purpose of internet use in school is to raise standards, to promote achievement, to support the professional work of staff and to enhance the school's management information and administrative systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Many children will access the internet both in school and outside of school and will need to learn how to evaluate online information and to take care of their own safety and security.

Aims
Through this policy we aim to:
- Safeguard and protect all members of Ellwood Community Primary School online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

As part of the curriculum, children will be made aware of the guidelines for the acceptable use of the internet. They will be taught how to use the internet responsibly and will always be given clear objectives when using the internet.

Ensuring Internet Access is Safe
The internet is used in school to support and enhance learning opportunities; it is part of the statutory curriculum and is a necessary tool for learning, both during and outside of school hours. During their time at Ellwood Community Primary School children will be educated in the effective use of the internet in research including the skills of knowledge location, retrieval and evaluation. It is also vital that they are fully equipped in knowing how to take care of their own safety and security whilst using the internet.

Just as with other media such as magazines, books and video, some material available on the internet is unsuitable for children. As a school we take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. However, due to the international scale and nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Instead, children will be suitably equipped to know how to react if the situation did arise.

Categories of risk

In her report, Professor Byron produced a simple table of risk categories which were originally defined by the EU Kids Online Project, and these are still used to a large extent today. These risk categories (sometimes referred to as the 3 Cs) allow us to talk about risk-based issues in a really simplified way:

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/ advice

The three C's:

Content: being exposed to illegal, inappropriate or harmful material
Contact: being subjected to harmful online interaction with other users
Conduct: personal online behaviour that increases the likelihood of, or cause harm.

The following measures have been adopted to help ensure that our children are not exposed to unsuitable material:

- Our internet access provides a service designed for children in a school setting, including a 'firewall' filtering system through SWGFL; intended to prevent access to material inappropriate for children.
- Children using the internet will normally be working in the classroom during lesson time and supervised by an adult. If children use the internet during lunchtimes, to plan collective worship for example, this will also be supervised by an adult.
- Staff will check that the sites pre-selected for the children to use are appropriate to the age and maturity of the children.
- If staff discover an unsuitable site, it will be reported to the class teacher and then to the School Business Manager who will inform our IT support technician who will subsequently ensure that the site is blocked. SWGFL will also be informed.
- Children will be taught to use e-mail and the internet responsibly in order to reduce the risk to themselves and others.
- Children will have access to information from relevant outside agencies.
Children using the school's computing facilities will be expected to comply with the above measures.

The Curriculum

The children are taught computing skills in line with the objective outlined in the National Curriculum. In order to specifically teach skills related to online safety we make use of the Digital Literacy and Citizenship resources provided by the SWGFL which covers the areas below in an age-appropriate way.

CROSS-CURRICULAR CATEGORIES

- Internet Safety
- Privacy & Security
- Relationships & Communication
- Cyberbullying
- Digital Footprint & Reputation
- Self Image & Identity
- Information Literacy
- Creative Credit & Copyright

Staff use of email

Email is an essential method of communication for educational settings, however, it can provide for unregulated contact from unknown individuals outside of the community. Spam, phishing and virus attachments can make emails dangerous. Therefore, **all staff and governors** must use their designated school email accounts to safeguard themselves and others.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images remain on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

Parents/Carers

Parents and carers are vital to teaching and empowering children to become safe and responsible digital citizens. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. We will therefore seek to provide information and awareness to parents and carers through:

- curriculum activities;

- letters, newsletters and website
- parents/carers information sessions
- participation in events such as Safer Internet Day.

Governors
We have a governor who is linked to computing throughout the school. Their role includes:
- liaising with the school regarding current practice in classrooms
- keeping up-to-date with online safety practices
- providing feedback to the Governing Body

The computing governor will be supplied with all the appropriate information on matters regarding online safety through meetings with the computing subject leader and through Governors' meetings.

This policy should be read in conjunction with the following policies:
Acceptable Use
Anti-Bullying and cyber-bullying
Behaviour
Complaints
Safeguarding and Child Protection
Data Protection
Equal Opportunities
Health and Safety
SRE

Policy written: January 2022