E-Safety Policy
2025-2027

Cecil Gowing Infant and Nursery School

Headteacher: Aimee Bulman
Chair of Governors: Julie Bennett

Review date: September 2027

Overview

To underpin the values and ethos of our school and our intent to ensure our children are appropriately safeguarded, this policy is included under the safeguarding umbrella. It also relates to the Computing policy.

What is E-Safety?

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones, games consoles, social networking and wireless technology. It highlights the need to educate all members of the school community, including children about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The safe and effective use of the Internet is an essential life-skill, required by all. However, unmediated Internet access brings with it the possibility of placing users in embarrassing, inappropriate and even dangerous situations. We set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.

The school's E-Safety coordinator is Sara Isaac. Our E-Safety Policy has been written by the school, building on best practice and government guidance.

It has been agreed by the teaching staff and approved by governors.

The e-safety policy and its implementation will be reviewed annually.

Every member of staff and regular helpers is provided with a Code of Conduct Guide that includes information for appropriate use of ICT.

Teaching and learning

Why Internet use is important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience and ensure children have a good understanding of how to keep themselves safe when using the internet.

How can we safely use the Internet to enhance learning?

The school Internet access is designed expressly for the use of pupils and will include filtering appropriate to the age of pupils.

Pupils will be taught in line with the computing curriculum about how it can be a useful and educational tool and how to keep themselves safe when using the internet.

Pupils will be taught how to evaluate Internet content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but despite filtering this is not easy to achieve and cannot be totally guaranteed. Through

guidance on safe computer use, children are told what to do if they see anything on the internet that they are uncomfortable with.

All online materials will be evaluated before use. The school will endeavor to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Information system security

The school has procedures in place to ensure that anti-virus and malware protection systems are installed and maintained on a regular basis.

Email

It is unlikely that children will be sending e mails individually and unsupervised. However, the following guidance should be followed:

- Pupils may only use approved e-mail accounts when supervised by a member of the teaching staff.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- 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.
- Staff should not contact pupils or parents using personal e mail addresses or social media in most circumstances.

Published content and the school web site

The contact details on the website are the school address, e-mail and telephone number. Staff or pupil personal information will not be published.

The ICT co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Photographing pupils and 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

Photographs that include pupils will be selected carefully and will not have names written on them.

Pupils' full names will not be used anywhere on the Web site or particularly in association with photographs.

Work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

The School will block/filter access to inappropriate social networking sites.

Staff must not access social networking sites for personal use via school information systems or using school equipment unless for a legitimate educational purpose.

Newsgroups will be blocked unless a specific use is approved.

If relevant, pupils will be advised never to give out personal details of any kind which may identify them or their location.

Staff should not communicate with parents or children using public social networking sites such as Facebook, Instagram, Twitter, etc. (When a member of staff is also a close friend of a parent any communication using social media must not included content referring to their role within school.)

It is inappropriate for pupils of primary age to use Social Network sites. However if children bring up the subject of social network sites, discussion will be encouraged so that children understand how to keep themselves safe on the internet, including on social networking sites in line with the Computing curriculum and the schools PSHE curriculum.

Any member of staff using social media should have their privacy settings on the highest level possible.

Managing filtering

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator or the Network Manager.

Managing emerging technologies

Children are not permitted to bring ICT devices into school, such as mobile phones or tablets unless there is an exceptional circumstance.

School staff should not use personal mobile phones and other personal ICT devices, during the school day, without the consent of the Headteacher.

Staff should not be contacting pupils or parents/carers using their personal devices unless there is an exceptional circumstance.

The sending of inappropriate messages by text or any other communication system or technology between any members of the school community is not allowed.

Parents are required to sign a consent form ensuing they understand that writing inflammatory comments about the school, staff and pupils on social media outlets is not tolerated. The school may need to seek advice from the LA if parents do write inappropriate comments.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Authorising Internet access

All staff must read the school E-safety policy before using any school ICT resource.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can not accept liability for the material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is effective.

Handling E-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be recorded and referred to the Headteacher. Safeguarding complaints must be discussed with the senior designated person and must be recorded and dealt with in accordance with school child protection procedures.

School website

- The school web site complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Communication

Introducing the E-Safety policy to pupils

Users will be informed that the Internet use will be monitored. Pupils will be given information so that they are better able to keep themselves safe when using information technology. Termly E-Safety assemblies will take place and each year group is required to include E-safety as part of their PSHE/Life Lessons curriculum. E-safety is fundamental part of the RHE objectives covered through the schools PSHE curriculum and taught within weekly Life Lessons.

Staff and the E-Safety policy

All staff will be shown the School E-Safety Policy and its importance will be explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Enlisting parents' support

Parents'/Carers' attention will be drawn to E-Safety in texts and on the website.

Parents/Carers will be directed to CEOP (Child Exploitation and Online Protection centre) in order to access one-stop shop website for internet safety and advice.

Tapestry

Tapestry is used throughout the school. Parents or carers sign an agreement before using, that outlines a code of conduct when using Tapestry. Parents will be supported by staff when accessing their child's learning journey.

Facebook

The school has its own Facebook page which is used primarily as an information tool about events at the school for current and prospective parents. It is maintained and monitored by staff within school. Parents are able to comment on Facebook posts. Parents are required to sign a consent form ensuing they understand that writing inflammatory comments about the school, staff and pupils on social media outlets is not tolerated. The school may need to seek advice from the LA if parents do write inappropriate comments.

Mobile devices and hand-held computers:

Mobile devices are not permitted to be used during school hours by pupils or members of staff. Staff may use their mobile devices in the staff room during breaks and lunches. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the E-safety officer when using these on the school premises. The sending of inappropriate messages or images from mobile devices is prohibited. Mobile devices will not be used to take images or videos of pupils or staff. The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.