UNIVERSITY OF CAMBRIDGE
PRIMARY SCHOOL

E-Safety Policy

Approved by
Education Committee

Last reviewed on	**Next review due**
September 2022	September 2024

RELEASING THE IMAGINATION:
CELEBRATING THE ART OF THE POSSIBLE

E-safety Policy: Safeguarding our Children

Introduction

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school focusing on:

- The ground rules we have developed in school for using the Internet, online technologies and handheld devices.
- How these fit into the wider context of our other school policies.
- The methods used to protect children from sites containing inappropriate content.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At University of Cambridge Primary School, we feel that the most successful approach lies in a combination of site filtering, supervision and fostering a responsible attitude in our pupils in partnership with parents/carers.

This policy (for all staff, governors, visitors and pupils) is inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, cameras etc.). Technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, cameras and portable media players, etc.), should also follow the same guidance.

Rationale

ICT in the 21st Century is seen as an essential resource to support learning and teaching and plays an important role in the everyday lives of children, young people and adults. Consequently, our school needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

It is 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 and Virtual Learning Environments
E-mail and Instant Messaging
Chat Rooms and Social Networking
Blogs and Wikis
Podcasting
Video Broadcasting
Music Downloading
Gaming
Mobile/ Smart phones with text, video and/ or web functionality

Other mobile devices with web functionality

The Risks

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

The use of these exciting and innovative technology tools has been shown to raise educational standards and promote pupil achievement, yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As part of our Prevent provision, we protect children from the risk of websites promoting radicalisation by supervising internet use and employing filters that make sure extremist and terrorist material is screened and not accessible.

The School's Responsibility

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

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction. Benefits of using online technologies in education include:

- Access to world-wide educational resources.
- Inclusion in the NEN (National Education Network) connecting all UK schools and resources.
- Access to a variety of E-safety resources.
- Access to experts who would otherwise be unavailable.
- Access to anytime, anywhere learning.
- Collaboration across schools, networks of schools and services.

Curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. At University of Cambridge Primary School, we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials.

Our programme for e-safety education is evidenced in teachers' planning and the Computing curriculum either as discrete or embedded activities. Members of staff constantly monitor pupils' use of the internet and other technologies and are able to monitor pupils' use of communication and publishing tools. Messages involving risks, rules and responsibilities are taught and/or reinforced as detailed in the school's Acceptable Use Policy.

Technology in our School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by the Local Authority's Education ICT Service. This helps to ensure that staff and pupils rarely encounter material or content which is inappropriate or offensive. If/when they do, the school's policies and e-safety education programme ensures that they are equipped to deal with the issue in an appropriate way.

All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password. Children have more limited access using the school logins and passwords.

The school's network can either be accessed using a wired or wireless connection however the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. School staff and visitors are permitted to connect personal devices to the school's visitor wireless network. Pupils are not permitted to connect personal devices to the school's wireless network.

Safeguarding Our Children Online

University of Cambridge Primary School recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school.

The school has published targeted Acceptable Use Agreements for pupils and staff to sign to indicate their acceptance of our Acceptable Use Policy and relevant sanctions which will be applied should rules be broken.

Any known or suspicious online misuse or problem will be reported to the designated E-Safety Co-ordinator and a Designated Person where necessary for investigation/action/ sanctions. The school will keep evidence and/or contribute to a log of any 'extreme' or 'unusual' actions that a pupil has been involved in online. This log will be used to keep track of the child's behaviours during the time they are at the school and will be stored alongside other incident or child protection logs. These are stored securely by the Head Teacher.

Responding to Incidents

It is important that all members of staff, teaching and non-teaching, are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. Responding to an e-safety incident in school is no different to responding to other incidents in school.

If an e-safety incident occurs, University of Cambridge Primary School will follow its usual procedures for dealing with other incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUP). Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

Dealing with Safeguarding Incidents and Seeking Help

If a concern is raised, staff will refer immediately to the designated person for child protection.
If that is not possible, refer to the team leader or, if necessary, the Chair of Governors.
It is their responsibility to:
Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator.
Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If you are in doubt consult the Education Child Protection Service:

Email: ECPSGeneral@cambridgeshire.gov.uk
Tel: 01223 729039
Fax: 01223 729056
Advice helpline: 01223 703800

Step 3: Ensure that the incident is documented using the standard child protection incident logging form.

Depending on the judgements made at steps 1 and 2, the following actions should be taken:

- Staff instigator; follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

- Staff victim; Seek advice from your HR provider and/or Educational Child Protection Service.
- Illegal activity involving a child; refer directly to Cambridgeshire Constabulary – 101 – make clear that it is a child protection issue.
- Inappropriate activity involving a child; follow standard child protection procedures. If unsure seek advice from Education Child Protection Service (contact details listed above).

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the usual procedures for dealing with any allegation against a member of staff.

Minimising Risk

At University of Cambridge Primary School, we carry out generic risk assessments as part of teachers' planning for the use of technologies and share these with the relevant groups e.g. staff, pupils and parents.