



E-Safety Policy

Approved by:

A handwritten signature in black ink, appearing to read "Alan Copple", is written over a white rectangular background.

Date: January 21

Last reviewed on: January 20

Next review due by: January
22

Acceptable use of the Internet policy for Cambridge School:

1. Introduction
2. School Policy
3. School Procedures
4. Staff rules for responsible internet use
5. Interactive whiteboard projector safety

1. Introduction

E - Safety Policy:

The Acceptable Use of the Internet and related Technologies

The aims of this policy and associated documents is to ensure the following areas are addressed in a manner that protects and guides all 'Stakeholders' in the use of Internet based technologies;-

- Managing the Internet safely
- Managing e-mail safely
- Using digital images and video safely
- Using the school network, equipment and data safely
- Infringements and possible sanctions

Context

Harnessing Technology: To Transform our Children's Learning, sets out the government plans for taking a strategic approach to the future development of ICT.

The Internet and related technologies are powerful tools, which open up new prospects and opportunities for communication and collaboration.

Cambridge School embraces these new technologies as they bring with them a range of approaches to education delivery for Teachers that enhances our children's education and promotes our school within the local community.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom. Organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school

These aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of our school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to our school's physical buildings.

GENERAL INTERNET ACCESS POLICY

The computer network is owned and run by the school and made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. This Internet Access Policy has been drawn up to protect all parties – the pupils the staff and the school.

- Cambridge School reserves the right to examine or delete any files that may be held on its computer system or stand-alone machines and to monitor any Internet sites visited.
- Any breach of this policy, by staff or pupils, will result in the right to Internet access being withdrawn and referral to the police where necessary.
- All Internet activity should be appropriate to staff professional activity or the pupil's education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT system, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Social networking sites are blocked at present in line with Lgfl policy.

2. Cambridge School Policy

This Policy document is drawn up to protect all parties – our / your Children, our staff and our school. The aims of which are: - to provide clear advice and guidance on how to minimise the risks and how to deal with any infringements.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements within Cambridge School:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive E-Safety education programme for pupils, staff and parents.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in our school and the Head Teacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for e-Safety has been designated to the safeguarding officer (Alan Campbell) who keeps up to date with E-Safety issues and guidance through liaison with the Local Authority E-Safety Officer (Hilary Shaw) and through organisations such as Becta and the Child Exploitation and Online Protection (CEOP).

The Governors have an overview understanding of E-Safety issues and strategies at our school and we ensure they are aware of our local and national guidance on E-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. Central to this is fostering a culture where pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school's policy including the staff and pupil rules for responsible internet use to include:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about E-Safety matters at least once a year. Access to on-line resources will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

The school provides an E-Safety education programme for pupils, staff and parents. The school provides many opportunities for raising awareness concerning staying safe using ICT. The subject is integrated into schemes of work.

3. School Procedures

Resource Development

In order to match electronic resources as closely as possible to the national and school curriculum, teachers need to review and evaluate resources in order to offer "home pages" and menus of materials that are appropriate to the age range and ability of the group being taught. It is the responsibility of **all** curriculum coordinators to ensure that the use of ICT is included in all curriculum policies and to keep up to date with developments of ICT relevant to their particular curriculum area(s).

All pupils will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

School Rules

The school has a set of guidelines for internet use by staff and pupils. The rules for staff use, given on the next page, must be read and adhered to by all staff. Any breach of these rules may lead to disciplinary procedures. All members of staff are responsible for explaining the rules and their implications to pupils. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Our school in conjunction with the L.A. monitors all computer activity and use.

This includes all types of text from word documents written to webpage's viewed, with infringements reported to the Head Teacher, after which Staff or pupil(s) concerned are given information about infringements in use and possible sanctions.

4. STAFF RULES FOR RESPONSIBLE INTERNET USE

This Internet Access Policy has been drawn up to protect all parties – the pupils the staff and the school.

- The school reserves the right to examine or delete any files that may be held on its computer system or stand-alone machines and to monitor any Internet sites visited.
- Any breach of this policy, by staff or pupils, will result in the right to Internet access being withdrawn.
- All Internet activity should be appropriate to staff professional activity or the pupil's education.
- Access should only be made via the authorised account and password, which should not be made available to any other person. Due to differing access rights staff should not allow pupils access to their user areas.
- Activity that threatens the integrity of the school ICT system, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

5. Interactive whiteboard projector safety

Use of interactive whiteboards with projectors is becoming increasingly common in schools. Certain precautions should be taken to avoid discomfort and possible damage to the eye. Training in the safe use of the equipment is essential.

Guidelines for Users of Computer Projectors

When using any form of data projector, the following guidelines should be adhered to.

- **Never stare directly into the projector beam.**
- **Keep your back to the beam as much as possible, and avoid standing facing into the beam for more than a few seconds at a time (the use of a stick or laser pointer* is helpful in this regard).**
- **Always step *outside* the projector beam when turning to face the class for more than a few seconds.**

Teachers should:

- **ensure that pupils are always adequately supervised whilst the projector is operating, and have been trained to follow safe routines of projector use.**

For any concerns regarding E – Safety please contact the School Business Manager r.moore@cambridge.lbfh.sch.uk