

Introduction

E-Safety is often defined as the safe and responsible use of technology. This includes the use of the internet and any other means of communication using electronic media (eg text messages, gaming devices, email, social media etc). Computing and ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Podcasting
- Coding
- Gaming
- Mobile devices
- Video & Multimedia
- Social media apps

E-Safety highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. Whilst these things can be exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

- E-Safety concerns **safeguarding** children and young people in the digital world.
- E-Safety emphasises **learning** to understand and use new technologies in a positive way.
- E-Safety is about **education** around the risks as well as the benefits so users can feel confident and safe online.
- E-Safety is concerned with **supporting** children and young people to develop safer online behaviours both in and out of school.

E-Safety in this context is classified into three areas of risk:

- **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 causes, harm.

The Internet is an unmanaged, open communications channel. The World Wide Web, email, blogs and social networks all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. At Hawthorn High 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.

Some of the material on the Internet is published for an adult audience and can include violent and inappropriate content. Information on weapons, crime, racism and extremism may also be unsuitable for children and young people to access. Pupils need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. The school has a duty of care to enable pupils to use on-line systems safely and appropriately.

The rapid development and accessibility of the Internet and new technologies such as personal publishing and social networking means that E-Safety is an ever growing and changing area of interest and concern.

The following apply to **all pupils** when using any information technology at Hawthorn High School:

1. Pupils should not use any form of information technology or use social media to cause distress or harm to others.
2. Pupils should not use the internet to search or display any content or information that could be deemed inappropriate.
3. Pupils should use the school internet and IT facilities for educational purposes which follow the teachers' instructions. This includes email, video, messaging, video-conferencing, social media, internet, file-saving and printing.
4. Pupils should not install software on school IT facilities due to the risk of damage being caused by malware or viruses.
5. Pupils should not share their network, internet or any other school-related passwords.
6. Pupils should change their passwords when asked to.
7. Pupils should only use their school-supplied email address for school-related activities.
8. Pupils should not look at or delete other people's work or files.
9. Pupils should make sure all their contact with other people at school is appropriate and responsible.

All internet activity within school is monitored and filtered through the security system. Whenever any inappropriate use is detected, the ICT Manager is notified and the incident will be followed up by the appropriate staff.

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day. The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

All users must report accidental access to inappropriate materials. The incident must be immediately reported to the teacher. Deliberate access to inappropriate materials by any user will lead to the incident being logged and investigated.

E-Safety Resources for Pupils

- BBC Advice
- CEOP (Child Exploitation & Online Protection)
- Childline
- Childnet International
- E-Safety for children and young people (Hwb resource)
- Kidsmart
- Pupil Support page
- School Beat
- Social Networks Checklist (Hwb Resource)
- Think U Know

E-Safety Resources for parents/carers

- CEOP (Child Exploitation & Online Protection)
- Childnet International
- Digital Dangers (Barnardo's resource)
- Digital parenting checklist (Vodafone resource)
- E-Safety for parents/carers (Hwb resource)
- Keeping children safe (NSPCC)
- Kidsmart
- Parent Info
- Parent Zone
- Digital parenting magazine (Parent Zone resource)
- School Beat
- Social Networks Checklist (Hwb Resource)
- Think U Know

Policy on the use of Mobile Phones and other electronic devices

(iPods, MP3 players, gaming devices or other electronic devices)

Pupils are permitted to bring electronic devices in to school but do so at their own risk.

The school does not allow the use of any of the above items during lessons. They have the potential to be used inappropriately by some pupils and can significantly distract from the teaching and learning in the lesson. Therefore the use of these items in class is treated as a serious offence.

The only exception, when electronic devices are permitted, is when they are used to enhance teaching and learning under the direct supervision of the class teacher.

Procedures

Pupils are not allowed to use mobile phones or any other electronic devices during lessons unless directed to do so by their teacher.

If a pupil is caught using any of these items they will be confiscated and handed into reception, parents/ carers will be contacted and the device can be collected by the parent/carer at the end of the school day.

If a device is confiscated from a pupil it should be handed into reception and entered on the pupil's record using the class charts behaviour system.