

Ellesmere Port Catholic High School

E-Safety

Status

Statutory

Introduction

The school is required to allow access to the internet for staff and pupils in order to provide education and associated functions. The internet is also be required to access school work at home and may also be used for students and staff to communicate.

Purpose

This policy is intended to ensure that digital device use is dealt with properly, fairly, securely and in accordance with the advice given by Child Exploitation & Online Protection Centre, Naace (National association for everyone promoting learning with technology in a connected world), internet providers and school rules. It applies to use of **all digital devices** (Desktops Computers, laptops, Tablets, Mobile Phones, Game consoles etc).

Relationship to Other Policies

The **Acceptable Use Policy** informs users (Staff and Students) of the rules of usage within the school environment. The **E-Safety Policy & Procedures** document produced by the Head of ICT and Computing (Appendix A). There are links also to **Behaviour, anti-bullying, personal, social and health education (PSHE)** and **for citizenship**.

Who/what was consulted?

This policy follows guidance issued by Government, CEOP and South West Grid For Learning with input from Students.

Roles and responsibilities of headteacher, other staff, governors

The **headteacher** will ensure that:

- The school has appointed an E-Safety Lead and CEOP Ambassador
- The E–Safety Policy and its implementation will be reviewed annually by the senior leadership team, staff, students and Governors.
- All staff dealing with internet usage attend training once every two years, in doing so are aware of the principles of e-safety, with written updates every term.
- Recording procedures are in place for the reporting of e-safety incidents/issues, with documentation being stored in a secure environment. Lead by Safeguarding lead and supported by Heads of year and E-safety Coordinator via CPOMS.

- The Acceptable Use Policy provided by the school is circulated to all new staff, parents and guardians of new entrants before enrolment.

Staff responsibilities

The **Business Manager** will be responsible for:

- Making the ICT communications and information systems Acceptable Use Policy available annually to all staff, for them to read and abide by.
- Ensuring filtering system is in place and monitored by site IT technicians and is appropriately identifying key violations within searches.
- Ensuring students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Passwords are changed every term to increase security to school systems.

Teaching and Support Staff are responsible for:

- Familiarising themselves with the Acceptable Use Policy and abiding by the policy.
- Ensuring students/pupils understand and follow the Online Safety Policy and acceptable use policies
- Encouraging every person including students to act responsibly when using the internet/digital devices by: leading by example and delivering clear instructions at the beginning of the lesson.
- Monitoring the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Reporting any incidents that are reported to them by any student or other member of staff, to the Safeguarding Lead or Head of Year via CPOMS.
- When using digital images, informing and educating students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

The **governing body** will ensure that:

- The e-safety policy is moderated, to ensure all terms and statements are clear and concise.
- Obligations are met by Safeguarding Lead, Heads of Year and E-safety Coordinator.
- Published on the school website is guidance on how to stay safe online and how to report any incidents in or outside of school environment.

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- must not take, use, share, publish or distribute images of others without their permission.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

Arrangements for monitoring and evaluation

The policy will be reviewed annually in the first instance. This will be over ridden on receipt of updates from the Government, CEOP, Naace, Internet provider, and school committee when the policy and procedures will be reviewed and updated immediately.

Signed on behalf of the Governing Body (Chair)



Date:

October 2018

Lead for Review

Head of ICT

Governor Review Committee

School Community

Date for Review:

July 2019