E-Safety Policy

Ellesmere Port Catholic High School

VERITAS ET SAPIENTIA

Approved by:	**Mr J Coucill, Chair of Governors**
Lead of Review:	**Mrs C Murphy, Careers & Personal Safety Lead**
Last reviewed on:	**October 2020**
Next review due by:	**September 2021**

Status

Statutory

Introduction

This policy applies to all members of Ellesmere Port Catholic High community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of *Ellesmere Port Catholic High School (EPCHS)*.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off EPCHS site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Ellesmere Port Catholic High School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

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.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing Body on: October 2020	*October 2020*
The implementation of this online safety policy will be monitored by the:	*Personal Safety Lead and Senior Leadership Team.*
Monitoring will take place at regular intervals:	*October 2020 (Every 12 months)*
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*October 2020 (Every 12 months)*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*October 2021*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Scie team, LA Safeguarding Officer, LADO, Police/CEOP*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students/students
  - parents/carers
  - staff

Roles and responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- regular meetings with the Personal Safety Lead
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Personal Safety Lead and other relevant staff receive suitable training in line with statutory changes each year to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Personal Safety Lead

The Designated Safeguarding Lead:

Should be trained in Online Safety issues (Safeguarding) and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Personal Safety Lead (Online Safety Lead)

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/MAT/relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical Staff

Those with technical responsibilities are responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required online safety technical requirements and any *Local Authority/MAT/other relevant body* online safety policy/guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy**
- *the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders*;* Personal Safety Lead; Pastoral Leader *f*or investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Other 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 ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the *Headteacher / Senior Leader; Online Safety Lead* for investigation/action/sanction
- all digital communications with students/parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities

- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor 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
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Reporting any incidents that are reported to them by any student or other member of staff, to the Safeguarding Lead or Pastoral Leader 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.
- **A planned programme of formal online safety training will be made available to staff. This will be updated and reinforced yearly in line with statutory changes. An audit of the online safety training needs of all staff will be carried out regularly**.
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.**

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.

The Online Safety Group:

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online

Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governors.

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents.
- the production/review/monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents / carers and the students / students about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

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/student records
- their children's personal devices in the school (where this is allowed)

Community Users:

Community Users who access school technology/website/Learning Platform as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems. This includes cover staff.