PHOENIX COLLEGE

E-SAFETY POLICY

Prepared by:	**Scott Versace**
Role:	**Senior Assistant Headteacher**
Approved by:	**The Full Governing Body**
Date:	**November 2017**
Next review due by:	**November 2018**

E-Safety Policy

Policy Statement

"In the context of inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the mechanisms in place to intervene and support any incident where appropriate."
Ofsted Inspection Briefing Document, 2013

Safeguarding is a serious matter. At Phoenix College we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

1. *To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met*.

2. *To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.*

This policy is available for anybody to read on the Phoenix College website.

All members of staff will sign as read and understood this e-safety policy, the more specific Staff Social Media Policy and the Staff Acceptable Use Policy. All three will form part of the Staff Induction Pack, given to new members of staff on appointment.
A copy of this e-safety policy, the more specific Student Social Media Policy and the Students Acceptable Use Policy will be included in the student pack sent to all new students accepted into the school.

Principal: Signed:
Chair of Governors: Signed:
Review Date: Next Review:

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that Phoenix College has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
  1. Keep up to date with emerging risks and threats through technology use.
  2. Receive regular updates from the Principal in regards to training, identified risks and any incidents.

The Principal

Reporting to the governing body, the Principal has overall responsibility for esafety within Phoenix College. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer, as indicated below.

The Principal will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The designated e-Safety Officer is devolved to*: Mr Scott Versace*

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize himself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Principal.
- Advise the Principal and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Make himself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Principal and responsible governor to decide on what reports may be appropriate

for viewing.

ICT Technical Support Staff – SOFTEGG

SOFTEGG is responsible for ensuring that:

The IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Software updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Principals.
- Passwords are applied correctly to all users.
- The IT System Administrator password is changed on a regular basis.

Teaching and Associate Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Principal.
- Any e-safety incident is reported to the e-Safety Officer (and an Incident report is written), or in his/her absence to the Principal. If you are unsure, the matter is to be raised with the e-Safety Officer or the Principal to make a decision.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy.

Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into the curriculum - students will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.

All students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have access to resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and the availability of free online training courses the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such all new parents will sign the student Acceptable Use Policy before their son can be granted any access to school network, ICT equipment or services.

Network and Device Management
Phoenix College uses a range of devices including PC's, laptops and tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering
The filter used at Phoenix College prevents the unauthorized access to illegal websites, including those sites deemed inappropriate under the Prevent Agenda. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ESafety Officer and IT Support (SOFTEGG) are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal.

Email Filtering
Email filtering prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. The system is also used to filter certain words and can be used for monitoring.

Passwords
All staff and students will be unable to access the network without a unique username and password. Staff and student passwords should be changed if there is a suspicion that it has been compromised. The network Manager will be responsible for ensuring that passwords are changed as and when required.

Anti-Virus
All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Principal if there are any concerns.

Safe Use
School Network & the Internet
Use of the school network, with access to the Internet, in school is a privilege, not a right.
Use will be granted to new staff upon signing of this e-Safety Policy, staff Social Media Policy, and the staff Acceptable Use Policy. All students will receive a copy of this E-safety Policy, the Student Social Media Policy and the Student Acceptable Use Policy. Access to the network will be granted to new students upon signing and returning their acceptance of the Acceptable Use Policy.
These policies apply to all staff and students whether access to the school network or internet is by cable or wireless (or personal mobile account whilst on school premises, including school trips) and on any device, laptop or PC, either school owned or personal.

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is expected to be used for professional work-based emails only. The use of personal email addresses for the purposes of contacting students is not permitted.
Students are permitted to use the school email system, and as such will be given their own email address, based on their network user name. Students should use this email account only for school based activity as laid out in the student Acceptable Use Policy that they have signed.

Photos and videos
All parents sign a photo release slip on entry to the school, as part of the Induction Pack they receive; non-return of the permission slip will not be assumed as acceptance.

Social Networking
Phoenix College is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Any subject specific social media services, permitted for use within Phoenix College, must have been appropriately risk assessed, managed and moderated in accordance with the Social Media Policies for Staff and Students.
In addition, with reference to images that may be uploaded to such sites, the following is to be strictly adhered to:

- Permission slips (either as hard copy filed in the student record folder or as flagged on the student record on SIMS) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used, if at all.

All images, videos and other visual resources that are not originated by the school are not allowed unless the owner's permission has been granted.

Permission to use copyrighted resources must be sought and received before they are used.

Notice and take down policy
Should it come to the schools attention that there is a resource which has been inadvertently uploaded, either to the school website or school/department authorized social networking sites, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Reporting E-safety Incidents
Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Principal. The e-Safety Officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log. All staff should make themselves aware of the procedures and the responsible staff involved in this process.

Training and Curriculum
It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this

includes updated awareness of new and emerging issues. This includes the regular distribution of e-safety information to staff, students and parents.
In addition, Phoenix College will have an annual programme of online e-Safety training for teaching/associate staff, to be incorporated within the CPD programme, with the Governors included. This online e-safety training provides staff with a certificate which must be renewed by further training on an annual basis. This continuous rolling training programme means that staff will always be up to date with the latest issues on e-safety from new and evolving technologies.
Phoenix College should ensure that aspects of e-Safety for students are firmly embedded into the curriculum. Whenever ICT is used in the school, staff will ensure that students are made aware about the safe use of technology and risks as part of the student's learning. If asked, staff should be able to demonstrate where and how the awareness of risk is imparted to students in lessons.
As well as the programme of training, the school will establish further training or lessons as necessary in response to any incidents.
The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Principal for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Principal for further CPD.

Policy approved by: Full Governing Body
Date: November 2017
Due for review: July 2018

Please refer to:
1 Acceptable Use Policy (Staff)
2 Social Media Policy (Staff)
3 Acceptable Use Policy (Students)
4 Social Media Policy (Students)