The Deanery
Church of England High School and Sixth Form College

E-SAFETY POLICY

MAY 2015

Aim
The E-Safety policy and procedures are to ensure young people use new technologies in a way which will keep them safe, without limiting their opportunities for creation and innovation.

Purpose
The Internet and digital communications are an essential element in the 21st century for education, business and social interaction. The school computer system and Internet access is designed expressly for student use and will include filtering appropriate to the age of the students. Clear boundaries will be set for the appropriate use of the computer system, the Internet and digital communications for staff and students.

Additional Relevant Policies and Procedures

- ICT Policy, which includes:
  Appendix 1 Acceptable Use Guidelines: Pupils.
  Appendix 2 Letter to Parents.
  Appendix 3 Acceptable Use Guidelines: Staff / Governors.
  Appendix 4 Action to be taken in the event of suspected abuse.
  Appendix 5 Network Induction Programme.
- Safeguarding policy.
- Bullying Policy.
- PSHE Policy.
- Scheme of Financial Administration(SOFA)- Relating to SIMS.
- Data Protection AC.

Requirements
All users of ICT within school must read and electronically agree that they have read and agree with the appropriate ICT Acceptable Use policy, once they agreed they system will allow them to logon.
All students and parents (Head of ICT Faculty)
Staff and Governors (Curriculum Deputy)

Staff Roles and Responsibilities

Role	**Responsibility**	**2012/2013**
E-Safety overview	Deputy Headteacher: Curriculum	D Farley
E-Safety monitoring	Technical: Network Manager Staff: Curriculum Deputy Sixth Form: Guidance & Welfare Officer Year 7 Pastoral Support Year 8 Pastoral Support Year 9 Pastoral Support Year 10 Pastoral Support Year 11 Pastoral Support Years 11-16: Pastoral Support	C Ellaby D Farley A Crowe B Robinson A Storey B Sullivan H Stockley K Boardman A Storey
Safeguarding	Assistant Headteacher	M Ryder
Student Guidance on ICT Use	Head of ICT	P Varey
Student Guidance	Headteacher, SLT, Progress Leaders, Teachers i/c SLS	Headteacher, SLT, Progress Leaders, Teachers i/c SLS
Staff	Ensuring E-safety when using technologies and communications	All staff

E-Safety Overview
Responsible for:

- Policy for E-Safety is written and regularly reviewed.
- Policy complies to all regulations regarding e-safety and safeguarding young people.
- Oversees all staff involved in monitoring.
- Following all policies related to E-Safety.
- Reporting serious issues to the relevant authority.
- Staff training on e-safety.

E-Safety Monitoring Technical
Responsible for:

- Ensuring that monitoring software is functioning correctly and set at an appropriate threshold level for each group of users.
- Following the procedures for system checks as listed.

E-Safety Monitoring Staff & Governors
Responsible for:

- Checking and following up all staff and governor alerts sent by the Impero software.
- Following all policies related to E-Safety.
- Reporting serious issues to the relevant authority.
- Deputy Head will receive alerts for inappropriate use by staff and appropriate action will be taken.
- Director of Resources will receive alerts for inappropriate use by support staff and appropriate action will be taken.

E-Safety Monitoring Sixth Form
Responsible for:

- Checking and following up all sixth form student alerts sent by the Impero software.
- Following all policies related to E-Safety.
- Reporting serious issues to the Curriculum Deputy and or Director of 6th Form as considered appropriate.

E-Safety Monitoring 11 - 16
Responsible for:

- Checking and following up all 11-16 pupil alerts sent by the Impero software.
- Following all policies related to E-Safety.
- Reporting serious issues to the Curriculum Deputy and or Director of Learning as considered appropriate.

Safeguarding
Responsible for:

- Following procedures specified in the policy.
- Reporting serious issues to the relevant authority.
- Recording incidents and the follow-up actions.

Student Guidance on ICT Use
Responsible for:

- Planning and delivery of lessons by the ICT department on E-Safety.
- Reporting serious issues to the relevant authority.

Student Guidance
SLT responsible for:

- Safeguarding young people.
- Annual assemblies on E-Safety.
- Annual assemblies on bullying (cyber-bullying).
- Annual assemblies on mobile phone use.
- Reporting serious issues to the relevant authority.

Head of SLS responsible for:

- Planning and delivery of lessons on e-safety.
- Planning and delivery of lessons on safety.

- Planning and delivery of lessons on bullying (cyber-bullying).
- Reporting serious issues to the relevant authority.

Staff
Responsible for:
- Monitoring use of technologies and communications in their lessons.
- Reporting serious issues to the relevant authority.

The school will provide anti-virus and filtering software on all computer access.

Systems Overview

Sophos Anti-Virus
The Sophos anti-virus product filters all computer traffic on the Deanery Network. It scans any file that is accessed on a student or staff machine for malicious programs that could infect files and render them inaccessible. It quarantines any suspect files found to prevent them spreading across the network and is logged and monitored by the Sophos Console that is checked on a regular basis by the network manager and technical staff for any warnings that may warrant intervention.

Suspicious Files
Sophos anti-virus, as well as scanning for viruses on the Deanery network, also checks for programs running on student or staff machines that may demonstrate suspicious behaviour. This prevents viruses or malware altering software on computers that could be used re-direct students to websites showing inappropriate content or stealing usernames and passwords. Any running program deemed suspect by the Sophos filter is logged on the Sophos Console and is checked by the technical staff to verify if the software is legitimate or rogue.

RM safety Net
All student internet traffic is passed through this filter and is scanned for access to websites deemed inappropriate by RM Safety Net or Deanery High School. RM Safety Net updates the blocked website list on a daily basis and currently has over 100,000 restricted websites; this database of sites can be added to or relaxed by Deanery technical staff. The filter also scans files and attachments downloaded from the internet or the email system for possible inappropriate content that could disrupt the network. All this information is stored in the filter for 30 days and is checked on a daily basis for inappropriate website access, attempts to bypass the filter or attempts to download files not allowed by the ICT policy in place at Deanery. Sites that should not accessible in school are manually blocked by the technical staff and this then gets uploaded to Sophos for review.

Impero Control
Impero is utilised by all ICT staff at Deanery and its primary function is to monitor student desktops in a classroom for either assisting by taking over a computer or preventing students accessing websites or material that they should not.

Impero
All curriculum and admin network activity is monitored by Impero software. This monitors all user activity and key strokes which are checked against library words and phrases. Where a violation occurs the software takes a screen shot or video of the users computer and e-mails the image to the appropriate person, (see previous tables).

Access
Access to the whole school network is available remotely through the web application portal. Staff and students can access their work folders, e-mail, Virtual Learning Environment (VLE) and the intranet. This access is still subject to the anti-virus and filtering software.

In addition staff can access SIMS remotely. Staff can only access SIMS remotely through a method which maintains security of the data. Staffs are required to lock their laptop away in a cupboard each evening if it is left in school. Staff may only carry sensitive data on mobile media devices which have been encrypted. Staffs have been made aware of the Data Protection Act.

This policy was reviewed and approved by the Curriculum Committee on 13th May 2015
Date of next review: May 2017