E-Safety Policy

SHOOTERS HILL
SIXTH FORM COLLEGE
Inspiring Young People

SHOOTERS HILL SIXTH FORM COLLEGE
Inspiring Young People

Shooters Hill Sixth Form College

Adopted and ratified by the Governing Body on:	**December 2016**
Review Date:	**September 2017**
Accountability:	**Governing Body**
Responsibility:	**Governing Body**

SHOOTERS HILL SIXTH FORM COLLEGE
Inspiring Young People

E-SAFETY INFORMATION

October 2015

1. IT Services Safety Guidance provided to Students at the start of the academic year.

   As part of each Students I.T induction, ALL students are informed that/they are;

   - Obliged to accept our Acceptable Use Policy (AUP) at the point of log-in.
   - Informed that their mobiles devices; tablets, iPads and Phones can connect to the student or guest Wi-Fi systems and that these are tracked and filtered via the SHC internet security policy.
   - Advised that all Campus devices auto connect to SHC Wi-Fi.
   - Advised that it is their personal responsibility to change and protect personal password(s) and that internet behaviour is recorded for each individual user.
   - Each time an inappropriate online search is attempted across any device using the SHC network this triggers an alert to I.T services. Once an individual triggers three alerts that person's name will appear at the top of our live negative-searches report and an automated email notification goes to the I.T services team summarising the users name, timestamp, computer and detail on the searches attempted. Typical trigger words and phrases include: guns, bombs, terrorism, pornography etc. IT Services will subsequently investigate that individual's full internet history and browsing log. This data will be recorded and reported on to the appropriate senior manager usually Student Services, Child Protection Officer or in the case of adults the HR Manager. This could lead to disciplinary sanctions.
   - Informed that Apps, Posters, software and advice is freely available from I.T. Services on e-safety, anti-bullying, social media, protection of personal data online and cyber risks to students.

2. Efficacy of the Campus Firewall & our Back-Up Strategy.

   The Campus I.T. Services Team has implemented a dual-firewall infrastructure, which means that we have a secondary firewall hidden behind the primary outward facing firewall. This provides a highly secure & protected internet filtering system, ensuring no malware; worms or email trackers enter the Campus domain. Although searches may be performed for inappropriate content using on–line search engines and results will be returned, the actual sites and their content will not be accessible.

   This provides Directors & Governors with confidence that students are secure when surfing on line and that they are protected from web-based risks and threats whilst using any I.T. resource on site. The Campus has implemented the BSI standards for IT best practice around internet safety and network security.

   This firewall also provides protection in the event of the failure of the primary firewall; the secondary system will automatically step in providing continuous protection. This introduces

what is referred to as a fully-redundant system. i.e. complete stability in the event of a system failure, as the secondary system assumes the primary function.

Shooters Hill Campus delivers a robust backup protection system and data protection system to all students and staff. The system takes a snap-shot at three intervals across each day [i.e. every file and folder within their personal work area is backed up. So even if deleted by a student we will be able to recover from live and archive versions of the backup. Students are not permitted to save certain file types or downloads, anything detected as a game or virus will be blocked by the system, if learning-related we advise staff and students to bring the data to IT services and we will assess the data.] This means that we can provide students with a backup file which is no more than 3-hours old. Backups are live for 14-days prior to moving onto a secondary system.

The final stage of protection is off-site data archiving and a Cloud-environment archive which is maintained for 5 years. This is all files and folders within their personal private allocated drive.

3. LRC & IT Services staff need further training in recognising potentially sensitive sites and how to identify individuals who are trying to use them.

   All Blocked/Disallowed sites that anyone tries to access are tagged prompting a negative mark against the particular students user account, which will show on reports for further investigation and evidence purposes.

   LRC and HUB staff are able to remotely monitor live student surfing activity and can take control of a student's screen should they be at risk.

4. Remote Teacher View
   All teachers have the facility to; view, monitor, remote control or freeze any or every student PC in any of the rooms they teach in. This allows a high-level of behaviour-management and I.T. control within each and every lesson. Further training on how to do this is scheduled for the Autumn term.

5. What to be aware of if students ask for help with research & how to assess whether a site is a cause for concern.

   Sites are categorised and alerts are triggered by content and key words. If a detected site is identified as potentially harmful or is suspected to contain negative content it will be blocked. Alerts will be sent to designated staff via the system and copied to I.T. Services staff monitoring activity.

   Searches performed by a student or staff member, using any search engine; Google, Yahoo, Bing etc. which trigger a system alert will not load up to the PC screen. The alert will trigger the system internally and be logged against the students username, this will also display within their

"blocked and disallowed" sites log. Therefore every search (allowed and blocked results), are marked against the user. This is further reiterated as part of the students IT induction.

Negative key-words, blocked sites and risk-categories are all marked against the person trying to access them, and will be visible via a series of detailed activity reports. All alerts are auto-logged to reports, prompting an action and view from a member of I.T. Services and thereafter to key staff including those with responsibility for Child Protection and Student Discipline. Staff need to be assigned to these key monitoring roles in order to provide further support in monitoring activity and student safeguarding.

Internet activity is monitored pro-actively to ensure that Campus users are not associating the organisation with any extremist organisations or their agendas, are not placing learners at risk and are not bringing the Campus reputation into disrepute.

6. What to do if you are working with students on sensitive research.

If the curriculum you are delivering is likely to introduce teaching or research which may generate cause for concern when you or your students perform internet searches, you will need to forewarn IT Services.

There are occasions when students need to research aspects of historical subject matter which trigger our monitoring systems such as War and Weaponry, Nazism, Holocaust Denial and Neo-Nazism, radicalisation etc.

If you are in any doubt about the nature of your curriculum you must discuss this with your line manager and advise IT Services or the Directorate accordingly.

Under no circumstances would it be appropriate to deliver content on the manufacture of weapons and incendiaries even under the banner of Chemistry and forensics.

Should a student either through their work, actions or demeanour lead you to suspect they have or are developing any kind of a radical agenda, are at risk of radicalisation or are vulnerable to grooming and other child protection issues, you must inform the safeguarding & child protection managers immediately.

If in doubt – Ask your line manager.

DfE Guidelines;

- Inclusion of reference to terrorist and/or extremist material within ICT code of conduct*, together with protections for legitimate study of this material.*

  Referenced in policy.

- Deliver awareness raising training to library and ICT colleagues about what terrorist and extremist material looks like.

- Raise awareness of colleagues and students or learners about updated code of conduct, reasons why and an explanation of how the policy was developed.

- Appropriate filtering is in place to ensure that learners are unable to access terrorist and extremist material online through college servers.

  As part of our e-safety and cyber-bullying programme of I.T projects, we have implemented a stringent and secure internet filtering and tracking system. The system blocks sites on category based filtering and key-words. Negative and Offensive alerts are recorded and tracked, which allow identification of at-risk students and repeat offenders, and deeper report generation as needed.

- Colleagues understand what terrorist/extremist material looks like and are confident to share concerns through the appropriate processes if they do encounter access to this material.

- Learner study of extremist and terrorist material for legitimate purposes is protected

  IT Services to review with Curriculum Managers as and when required.

- Students and learners understand the risks attached to accessing terrorist and extremist material online and understand the institution's duty and process in these areas

  This is outlined within each student I.T induction session.

  Students are informed that ALL their internet behaviour and activity is tracked and monitored. This is done in-line with the students I.T. Acceptable Use Policy (AUP), and across ALL Campus and Personal devices connected to the SHC Wi-Fi system.

  Learners are safe from accessing extremist or terrorist materials whilst using Campus servers.

  A secure and live safeguarding service is delivered to all SHC students and staff. This is done through implementation and management of secure firewalls and conducting of monthly penetration testing on the Wi-Fi and internet service for all students and staff.

SHOOTERS HILL
SIXTH FORM COLLEGE
Inspiring Young People