Shoeburyness High School

A member of Southend East Community Academy Trust

E-Safety Policy

May 2018

Status	:	Statutory
Next revision due	:	May 2019
Reviewed and monitored by	:	CPDL Business and Computing
Approved by	:	Local Governing Body
Signed by Chair of the Local Governing Body	:	

1. RATIONALE & PURPOSE

The purpose of the School E-Safety Policy is to:

- Clarify the legal requirements and responsibilities of the school.
- Protect and safeguard the health and safety of pupils and others who use the school.
- Clarify the school's approach to e-safety for all staff, parents, governors, parents/carers, outside agencies, volunteers and the wider community.
- The school will play its part in helping pupils and students meet the opportunities and challenges of childhood, adolescence and adult life. This includes E-Safety and Cyber Bullying.
- Enable staff to respond to e-safety concerns with confidence and consistency and in the best interests of those involved.
- In response to our shared concerns at a local and national level, we wish to state that as part of its care for the welfare of its pupils, Shoeburyness High School believes it has a duty to educate its students on the potential risks of online activities and digital equipment. We take a pro-active stance on this matter, believing that staying safe online is an integral part of the ICT and Personal, Social and Health Education (SCOPE) of every student.

This school:

a) Understands the importance of e-safety as a part of safeguarding and has invested in training members of staff in e-safety training through the Child Exploitation and Online Protection (CEOP) 'Thinkuknow' training and Prevent online training. Their job is to keep informed about the latest technologies, the threats they may pose and to cascade awareness and deliver training to students, staff, governors and parents.

b) Is vigilant in its supervision of pupils' use at all times, as far as is reasonable and uses common-sense strategies in learning resource areas where older pupils have more flexible access.

c) Ensures all students have signed an acceptable use agreement form and understand that they must report any concerns.

d) Ensures all staff sign an acceptable use agreement before gaining access to the schools VPN (Virtual Private Network).

e) Ensures pupils only publish within the appropriately secure school's learning environment, such as the VPN.

f) Requires staff to preview websites before use [where not previously viewed] and encourages use of the school's email as a key way to direct students to age / subject appropriate web sites.

g) Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.

h) Informs users that Internet use is monitored.

i) Informs staff and students that they must report any failure of the filtering systems directly to the *ICT Technical Team.* If any sites or web locations need to be filtered then this information is added into our web filtering software via Smoothwall.

j) Requires pupils to individually sign an acceptable use agreement form which is fully explained and used as part of the teaching programme.

k) Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the acceptable use agreement form at the time of their child's entry to the school.

l) Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse (this varies depending on misuse) – through staff meetings and teaching programme.

m) Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system.

n) Ensures the named child protection officer has appropriate training.

o) Provides advice and information on reporting offensive materials, abuse/ bullying etc, available for pupils, staff and parents.

p) Provides e-safety advice for pupils, staff and parents/carers; Ongoing training for staff and governors is a priority, awareness sessions are advertised to parents at parents consultation evenings and links to CEOPS and other advisory sites are advertised through the schools website. In house training and information materials are available to staff.

q) Will immediately refer any material we suspect is illegal to the appropriate authorities i.e. the Police and the Local Authority (LA).

r) Will carry out regular e-safety information risk assessments and inform the Senior Team and Governors of any significant change in risk to data security as a result.

s) Will promote the Prevent programme/duty as part of its e-safety duty with regard to the use of social media (and other means) for online radicalisation.

t) Will promote the safer use of the internet and online content through various national programs e.g. Safer Internet Day.

2. POLICY STATEMENT

This school:

Tries to ensure that the use of technology by staff and students alike does not contravene any of the following acts:-

- Racial and Religious Hatred Act 2006
- Sexual Offences Act 2003
- Communications Act 2003 (section 127)
- The Computer Misuse Act 1990 (sections 1 - 3)
- Malicious Communications Act 1988 (section 1)

It does this because it:

a) Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable.

b) Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.

c) Ensures pupils and staff know what to do if there is a cyber-bullying incident; New staff receive mandatory training, many existing staff have received CPD e-safety training and others are aware of imminent training videos available on the Staff pool drive.

d) Ensures all pupils know how to report any abuse.

e) Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA and national guidance. In Computing, SCOPE and assemblies pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

   - to STOP and THINK before they CLICK ;
   - to discriminate between fact, fiction and opinion;
   - to develop a range of strategies to validate and verify information before accepting its accuracy;
   - to skim and scan information;
   - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
   - to know how to narrow down or refine a search;
   - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;

- to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- will not send inappropriate pictures of themselves to anyone, even boy/girlfriends, sexting is a growing concern among KS4 and KS5 and as such is a priority topic for assemblies;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- to understand the age restrictions on video games and the reason behind these restrictions using the PEGI (Pan European Game Information) system.

f) Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.

g) Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.

h) Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

i) Makes training available regularly to staff on the e-safety CPD (continuing professional development) education program.

j) Runs as requested sessions of advice, guidance and training for parents, including:
   - Information leaflets; in school newsletters; on the school web site; demonstrations, practical sessions held at school;
   - direction to 'think u know' for parents materials;
   - suggestions for safe internet use at home;
   - provision of information about national support sites for parents.

3. GUIDING PRINCIPLES

The school strives to ensure that all users:

a) Take responsibility for their own use of communication and interactive technologies, making sure they use new technologies safely, responsibly and legally.

b) Do not use any communication device or service including social networking, to bring the school into disrepute.

c) Can identify sources of appropriate personal support.

4. CONSULTATION GROUP

- CPDL Business and Computing
- E-Safety Trained Staff
- Deputy Headteacher
- Network Manager

5. LINKS TO OTHER POLICIES & DOCUMENTS

- Safeguarding
- Anti-Bullying
- Child Protection
- Behaviour
- PSHE
- Students IT Acceptable use contract
- Staff ICT Acceptable Use Policy
- IT Security Policy

6. MONITORING & EVALUATION ARRANGEMENTS

The implementation of this e-safety policy will be monitored by the E-Safety Ambassador at termly intervals or more regularly in the light of any significant new development in the use of the technologies, new threats to e-safety or incidents that have taken place.

This E-Safety Policy will be reviewed annually by the Governing Body.

7. ROLES & RESPONSIBILITES

The CPDL Business and Computing is responsible (with other trained e-safety staff) for delivering/co-ordinating staff training and updates on e-safety issues.

All staff are expected to adopt the schools consistent approach to the safe use of technology and report any e-safety concerns to the relevant staff.

APPENDIX I PROCEDURES

Any concerns should be reported directly to one of the designated senior child protection people in the first instance who will then ensure the concerns are investigated.

This school:

- Has the educational secure broadband connectivity through the E2BN and so connects to the 'private' National Education Network;
- Uses the Smoothwall Secure Web Gateway which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses group-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures the network health through use of Sophos anti-virus software etc., and network set-up so staff and pupils cannot run unauthorised files;
- Uses DfE, LA or E2BN approved systems for secure remote access via our Cisco ASA (Adaptive Security Appliance) and Bromcom Webfolder where staff need to access personal level data off-site;
- Blocks all chat rooms and social networking sites (where possible) except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- As far as possible blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level;
- Uses security time-outs on internet access where practicable / useful;
- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and internet web sites, where useful;
- Works in partnership with the LA to ensure any concerns about the system are communicated so that systems remain robust and protect students;

Ensures the Systems Administrator / network manager is up-to-date with LA services and policies.

APPENDIX II DEFINITIONS

Cyberbullying: Bullying via a digital medium.

Sexting: Sending sexual images of yourself or others over a digital medium.