****

**eSafety Policy**

**December 2015**

|  |  |
| --- | --- |
| School Staff were consulted on this document and it was accepted by the standard & performance committee on : |  |
| It was ratified by the Governing Body on : |  |

**Introduction**

This e-safety policy has been developed primarily by Jenny Comerford (Deputy Head Safegaurding) and DJ Barron in liaison with a working party made up of:

* Senior Leaders
* E-Safety Officer / Coordinator
* Staff – including Teachers, Support Staff, Technical staff

Consultation with the whole school community has taken place through a range of formal and informal meetings. The policy is disseminated to staff through specific Esafety training and general safeguarding training, it also forms part of induction of new staff.

Creating a safe ICT learning environment consists of three main elements at Shenfield High School:

* Education about and access to e-Safety information for students, staff, parents/guardians and other users.
* Clear policies and procedures including roles and responsibilities.
* An effective range of technological tools to monitor and restrict computer/internet access (Ranger and light speed web filtering).

**Review Procedure**

There shall be on-going opportunities for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them. A designated Esafety email exists ([safety@shenfield.essex.sch.uk](mailto:safety@shenfield.essex.sch.uk)) which allows the prompt communication of any concern and also act as record keeping. Issues that might lead to a review of the policy are discussed regularly as part of the school’s Safeguarding Board meetings.

The policy shall be amended if new technologies are adopted or Government change the orders or guidance in any way.

This policy has been read, amended and approved by staff, the Head Teacher and Governors on XXXX

It has been agreed by Jenny Comerford (Deputy Head: Student Wellbeing and Support) and the Governors that the policy shall be reviewed every year and/or after any serious incident.

The impact of the policy will be monitored by:

* Logs of reported incidents
* Monitoring logs of internet activity (including sites visited)
* Internal monitoring data for network activity
* Surveys / questionnaires of:

students / pupils

parents / carers

staff

**Scope of policy**

This policy sets out the school’s expectations of all members of the *school* community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of the school *.* This policy is designed to express the school’s philosophy and vision with regard to the Internet, VLE and electronic communication in general. It aims to set general principles users should apply when using the services at the school, but this guidance cannot and does not attempt to cover every possible situation.

**Responsibilities**

The primary responsibility for e-safety is first and foremost with the person using ICT equipment. Students and staff have a responsibility to follow the guidelines agreed to in this policy and the Acceptable Use Policies and to avoid as best as possible situations that put them at risk.

The Head and Governors have ultimate responsibility to ensure that the policy and practices.

This policy, supported by the school’s Acceptable Use Policies, protects the interests and safety of the whole school community. It supports the following mandatory school policies: Child Protection, Health and Safety, home–school agreements, and behaviour / student discipline (including the anti-bullying) policy and PHSE.

**Governors / Board of Directors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor . The role of the E-Safety Governor / Director will include:

• regular meetings with the E-Safety Co-ordinator / Officer.

• regular monitoring of e-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 e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

• 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 e-safety allegation being made against a member of staff.

• The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

**E-Safety Coordinator**

The named e-Safety co-ordinator in our school is DJ Barron who works in collaboration with **Jenny Comerford and other members of the Schools Safeguarding Board** . The e-safety co-ordinator:

• leads the e-safety committee.

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

• provides training and advice for staff.

• liaises with the Local Authority / relevant body in collaboration with safeguarding lead

• liaises with school technical staff.

• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

• meets regularly with E-Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meetings with *Governors*

• reports regularly to Senior Leadership Team

**Network Manager / Technical staff**

The Network Manager and technical staff 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 e-safety technical requirements and any Local Authority guidance that may apply.

• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

• the filtering system 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 e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

• that the use of the network (including, internet, Virtual Learning Environment, remote access and email) regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Principal / Senior Leader; E-Safety Coordinator for investigation.

• that monitoring software / systems are implemented and updated as agreed in school policies.

**Teaching and Support Staff**

Are responsible for ensuring that:

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

* Any staff that use portable storage devices that stores sensitive school data shall have a password to protect the data in the event the storage device is lost or stolen.
* Work that is stored on either a school laptop or a laptop at home that stores any sensitive data from work shall be password protected in the case of the data being lost or stolen.
* Staff should not accept students or parents as friends on social networking websites until there is no longer any professional responsibility for the student (when the student has left the school). Even when there is no longer any professional responsibility, accepting a student or parent on a social networking site is still strongly not advised and potentially puts the member of staff at risk.
* Any images that have been taken of students using either a camera or video camera shall be removed from the camera and stored on the computer system within school and not anywhere else. Staff need to take particular care accessing icloud features on their school ipad. Particular element of icloud sharing (or similar online file sharing facilities) must be disables so that sensitive information relating to students or the school are not accessible on a similar device outside of the work environment.
* When sending parents or students an email, staff must only use the schools email system. Staff must not give out their own personal email address. If a member of staff receives an email that is offensive in any way they need to notify the e-Safety officer or a senior member of staff so that the matter can be investigated further.
* Staff should not investigate any e-safety concerns themselves. If a student’s activity poses a risk it should be stopped the details passed on immediately to the Head teacher, Senior Leader or e-safety officer.

**Child Protection / Safeguarding Designated Officer**

Should be trained in e-safety issues 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

• cyber-bullying

**Safeguarding Group**

The Safeguarding group provides a consultative group that has wide representation from the *school* community, with responsibility for issues relating to safeguarding. The group will also be responsible for regular reporting to the Governing Body.

Members of the Safeguarding group will assist the E-Safety Coordinator with:

• the production / review / monitoring of the school e-safety policy / documents.

• the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.

• mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression

• monitoring network / internet / incident logs

• consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision

• monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students / pupils

**•** are responsible for using the *school / academy* digital technology systems in accordance with the Student / Pupil Acceptable Use Policy

• 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 e-safety practice when using digital technologies out of school and realise that the *school’s*  E-Safety Policy covers their actions out of school, if related to their membership of the school

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 and information about national or local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-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 / VLE and on-line student / pupil records

• their children’s personal devices in the school / academy (where this is allowed)

**Investigations and concerns**

11

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to e-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.

The 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 e-safety behaviour that take place out of school.

If a member of the school community suspects another of viewing or using inappropriate or illegal ICT, it must be reported to the Senior Leader of the school, for example the Child Protection Officer or member of the Senior Leadership Team. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source, or asking student’s to open something on their account. This puts the person accessing at incredible risk and images or content that is accessed is potentially illegal meaning the person accessing the material will have committed an offense. Any allegation of inappropriate behaviour must be reported to the Senior Leadership Team and investigated with care. Advice should be sought from the Designated Officer for Child Protection and / or Essex Police.

No policy can protect students without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. The following suggestions may be useful:

* e-Safety awareness is an essential element of all staff and volunteer induction.
* The audit tool provided in the Core e-Safety Policies is a good place to start when checking the school’s e-Safety readiness
* Students should be reminded of their responsibilities whenever they are using the Internet. Displaying and referring to posters in rooms with Internet access is one useful approach.
* Ensure all staff, students and parents know how to report an incident of concern regarding Internet use.
* Make sure a member of the senior leadership team (if filtering is managed locally) approves the school filtering configuration and supervise the staff who manage the filtering system.

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

• Erase or amend data or programs without authority;

• Obtain unauthorised access to a computer;

• “Eavesdrop” on a computer;

• Make unauthorised use of computer time or facilities;

• Maliciously corrupt or erase data or programs;

• Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

• Fairly and lawfully processed.

• Processed for limited purposes.

• Adequate, relevant and not excessive.

• Accurate.

• Not kept longer than necessary.

• Processed in accordance with the data subject’s rights.

• Secure.

• Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

• Establish the facts;

• Ascertain compliance with regulatory or self-regulatory practices or procedures;

• Demonstrate standards, which are or ought to be achieved by persons using the system;

• Investigate or detect unauthorised use of the communications system;

• Prevent or detect crime or in the interests of national security;

• Ensure the effective operation of the system.

• Monitoring but not recording is also permissible in order to:

• Ascertain whether the communication is business or personal;

• Protect or support help line staff.

• The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

• The right to a fair trial

• The right to respect for private and family life, home and correspondence

• Freedom of thought, conscience and religion

• Freedom of expression

• Freedom of assembly

• Prohibition of discrimination

• The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

51

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - <http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations>

This policy has been reviewed by Jenny Comerford and DJ Barron

E – safety link Governor – Mrs Jane Swettenham

Ratified by the Governors – XX

Next review date – XX