

**Esafety**

 **Policy**

|  |  |
| --- | --- |
| School Staff were consulted on this document and it was accepted by the standards and performance committee on : | **September 2018** |
| It was ratified by the Governing Body on : | **November 2018** |

**Introduction**

Esafety is *“the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, Infrastructures and education, including training, underpinned by standards and inspection (source BECTA. BECTA was closed by the coalition government 31st March 2011).”*

IDTMs are seen as an essential resource to support teaching and learning within school, as well as playing a role in the everyday lives of young people and adults. The school needs to build in the use of these technologies to prepare our young people with the skills to access life-long learning and employment. It is also important to recognise the constant and fast paced evolution of IDTM within our society as a whole.

At Shenfield High School***,*** we understand the responsibility to educate our staff, parents, students and governors on e-Safety issues; informing every one of the most up to date guidance available through staff and governor training, parent workshops and students through, assemblies and the curriculum.

This e-safety policy has been developed primarily by Safeguarding Leads, in liaison with

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

The policy has been written with particular reference to *‘Sexting in schools and colleges: Responding to incidents and safeguarding young people”* produced by the UK Council for Child Internet Safety, Keeping Children Safe in Education and referencing the E-Safety Policy suggested by Essex Safeguarding Children Board.

This policy sets out the school’s expectations of all members of the *school* community (including staff, students, 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 includes accessing wireless 3G and 4G, remembering that any site accessed or any information sent or received whilst on school site is subject to the same scrutiny as data that is accessed via our wifi systems.  This includes social media, what is said and sent and data that is accessed and downloaded.  The user agreements for both staff and for students makes this expectation very explicit, and means that consequences for breaking expectations will be used.

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 learning environment that embraces the use of new technology consists of four 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.
* Acceptable use agreements
* An effective range of technological tools to monitor and restrict computer/internet access

**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) which allows further lines of communication and record keeping , which sit alongside existing safeguarding systems.

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 to keep up-to-date with contemporary technology and user platforms, as well as to reflect current legislation and Government guidance.

It has been agreed by the Governors that the policy shall be formally reviewed every year or in the event of any in year incident that requires a review.

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
* Stakeholder voice
* Governor monitoring visits

**Responsibilities**

The primary responsibility for e-safety is first and foremost with the person using IDTM equipment. Users 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 Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are followed.

This policy, supported by the school’s Acceptable Use Policies, protects the interests and safety of the whole school community. It supports the following school policies: Safeguarding, Health and Safety, Staff Code of Conduct, Acceptable use Agreement home–school agreements, and Behaviour for Learning (including the anti-bullying) policy and PHSE (including the assembly and form time programme).

**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 through safeguarding up-dates and monitoring visits. E safety is monitored by The Standards and Performance Committee and, in particular, by the Safeguarding Lead Governor. Through the work of this Committee and also via Governor monitoring visits, Governors will have:

• regular updates from the E-Safety Officer.

• regular monitoring of e-safety incident logs.

• regular monitoring of filtering / change control logs.

In addition, any incidents that require policy review and change will be reported in the Safeguarding Update and annual report to the governors by the Safeguarding Lead at Full Governing Body meetings.

 **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 Safeguarding Leads 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 one of our Designated Safeguarding Leads who works in collaboration with **our three other Safeguarding Leads and other members of the School’s Safeguarding Board** . The e-safety co-ordinator:

* takes strategic responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
* consults stakeholders – including parents / carers and the students / pupils about the e-safety provision.
* ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. (see appendix 3)
* provides training and advice for stakeholders.
* 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 the Safeguarding Lead to discuss current issues, review incident logs and filtering / change control logs, who will ensure that all relevant information is passed onto The Standards and Performance Committee and where relevant, the Full Governing Body.

**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. However, the E Safety lead also works with technical staff to ensure that the filtering system does not throw out everything, because there is a strong emphasis on all adults helping children and young people to engage with the internet in a safe and discerning manner, learning how to keep themselves and other children and young people safe online.

• 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 expectations are laid out in the Staff ICT Acceptable use policy (appendix 1)**

Students responsibilities are outlined in the ICT acceptable use statement for students (appendix 2)

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 (see Photography at School events policy)

• access to parents’ sections of the website and Go4Schools.

• their children’s personal devices in the school (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 for Learning 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 material, it must be reported to the safeguarding lead, and where the member of the school community so suspected is an adult, to the Headteacher or the Chair of Governors. This point is supported by the school’s Whistleblowing Policy, and people in this position can also find support on Whistleblowing via the NSPCC website.

Any allegation of inappropriate behaviour must be reported to the Safeguarding Lead, the Headteacher and/or the Chair of Governors and investigated with care. Advice should be sought from the Designated Officer for Safeguarding and / or Essex Police by calling 101, and/or the Essex Family Operations Hub by calling 0345 603 7627, and/or by contacting the NSPCC via their website - <https://www.nspcc.org.uk/fighting-for-childhood/about-us/contact-us>

In line with advice ascertained from ESCB (Essex Safeguarding Children Board) and Police authorities, any form of investigation into misuse of technology must align directly with school procedures. This may include incidents such as ‘Sexting’ or the sharing of inappropriate images via mobile and technological devices.

This policy has been reviewed by the safeguarding leads, the Safeguarding Board and staff as a whole during the consultative period.

Ratified by the Governors – XX

Appendix 1: Staff Acceptable Use Policy

This covers the use of all *Internet, Digital and Mobile Technologies (IDTMs)* within school or connected to the school network in anyway.

Security

* I will only use IDMTs for professional purposes or for uses deemed ‘reasonable’ by the Head and governing body.
* I understand that it is a criminal offence to use a school IDMT for a purpose not permitted by its owner
* I will not browse, download or send material that could be considered offensive to any stakeholders
* I will report any accidental access to, or receipt of inappropriate materials, or filtering break to IT Support
* I will not allow unauthorised individuals to access email/internet/network or other school systems. I will lock my computer when away from it
* I will not disclose any password or security information to anyone.
* I will not download any software or resources form that internet that compromise the network or are not adequately licensed.
* I will not connect any device to the network that does not have adequate security settings
* I will report any colleague who fail to meet these standards.
* I will report any incidents of concern regarding children’s safety or behaviour when using IDMTs in line with the schools safeguarding policy.
* I will stop any inappropriate use of IDMTs and confiscate the device in line with policy but I will not investigate Esafety concerns myself, either by looking on stakeholders personal IDMTs or taking copies of ‘evidence’
* I will ensure any confidential or identifying data is protected and stored securely. Any IDMT used to access such data offsite will be encrypted and/or password protected.
* I will endeavour to use the school provided IDMTs when recording or creating images of a stakeholder. If for practical reasons this is not possible I will remove any images from a personal device to the school system

Communication

* I will only use the approved, secure email system(s) or school endorsed systems for any school business or communication with stakeholders
* I will ensure any private social networking sites or internet profile I create or actively contribute to are not confused with my professional role or reflect negatively on the academy, its staff or the profession.
* I will not engage in any online activity that may compromise by professional responsibilities
* I will not accept current stakeholders on private social media account, and understand that accepting former students leaves me open to questions of when that ‘relationship’ formed.

I understand that failure to comply with the acceptable use policy could lead to disciplinary action, and if appropriate, Police or other authorities will be involved and criminal proceedings may be instigated.

Signature Date

Full Name

Appendix 2: Student acceptable use policy

At Shenfield High School it is our priority to keep students safe at all times, this includes when using Information Digital Mobile Technologies when on site or connected to the school network. As a member of SHS you must use such devices in with the acceptable use policy below:

1. I will treat all IDMT with respect and I accept responsibility or any damage caused
2. I will use the school’s network, software and devices only for activities agreed by a staff member
3. I will not share my passwords with others
4. I will only attempt to communicate with staff members through the school provided systems
5. I will not attempt to access or download any software to the school system
6. I will not accept, download or share any offensive or illegal content using any IDMT on school site or connected to the network
7. I will not attempt to access any area that is protected by restricted permissions
8. I am responsible for my online behaviour, including the use of resources and language used
9. I will respect the privacy and ownership of other people’s work
10. I will uphold the academic/scholastic principles of anti-plagiarism
11. I will not use any IDMT to create images, videos or audio that reflect poorly on the school, staff or students. Any recording linked with Shenfield High School are not to be shared or distributed without the school’s permission.
12. My online activity, inside and outside Shenfield High School, will not cause distress to others. I will not bully anyone online.
13. I will inform an adult immediately if I see someone not following the rules outlined above or I see something online that makes me feel uncomfortable
14. If I need to use a IDTM, this will only be done with teachers permission, in the designated areas at the designated times.

I understand that my use of the network is monitored and that nothing posted online is ‘private’. As such information can be made available to my teachers, parents/carers and/or the police. I understand these rules are there to keep me safe. I understand that consequences will be applied and my parents/carers will be informed if I fail to abide by this Acceptable Use Agreement.

Signed: Date:

**Appendix 3 - investigations**