EDUCATION SOUTH WEST

E Safety Policy

Board Approved Date	October 2021
Version	0.3
Author Initials	MS/DP
Review Date	October 2023

(This policy supersedes all previous E Safety Policies)

Amendments

Policy Date	New Version Number	Summary of change	Comments
091019	0.2	1.2 All staff to adhere to use of social media policy. 6.11/12 Expanded to include ESW Shared Services team 7.2 Safeguarding staff using school social media	
02 10 2021	0.3	Safeguarding Monitoring (Securus) Added Sec. 6	

Contents

1. Introduction..3
2. Policy..4
3. Education / Training / Awareness...5
4. Online bullying..5
5. Internet Filtering..6
6. Key steps in the process...6
7. Procedures..11
8. Local conditions statement...12

1. Introduction

Statement

1.1 Education South West believes that online safety is an essential element of safeguarding children and adults in the digital world. The internet and information communication technologies are now an important part of everyday life so children must be supported to develop strategies to manage risk so to empower them to build resilience online.

1.2 The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. All staff should use social media in accordance to the ESW Social Media Policy.

Aim and purpose

1.3 Education South West has a duty to provide quality Internet access to all areas of the school to raise education standards, promote student achievement, support professional work of staff and enhance management functions. Education South West also identifies that with this there is a clear duty to ensure that children are protected from potential harm online. This policy should be read in conjunction with the Anti-Bullying Policy, the ICT Misuse Policy, the Social Media Policy and the Video and Digital Image Policy.

Who it applies too

1.4 All ESW staff, volunteers, Local Governing Board and Director Members, visitors, community users and contractors.

2. Policy

Description

2.1 All members of the school's community are encouraged to engage in social media in a positive, safe and responsible manner. Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school's community.

Internet Filtering

2.2 Internet access is filtered for all users. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context.

- Differentiated internet access is available for agreed groups of users (see below) and customised filtering changes are managed by the ESW IT Services Team
- Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists
- Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.
- There is a clear route for reporting and managing changes to the filtering system
- All users have a responsibility to report immediately to the ESW IT Services Team any infringements of the trust's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered
- Users must not knowingly attempt to use any Programs, software or external resources such as VPNs which may allow them to bypass the filtering / security systems in place to prevent access to such materials

3. Education / Training / Awareness

3.1 Pupils will be made aware of the importance of filtering systems through teaching the computing curriculum.

3.2 Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, inset.

3.3 Parents will be informed of the trust's filtering policy through the Acceptable Use agreement and through online safety awareness sessions / newsletter.

4. Online bullying

4.1 We take any incident of online bullying extremely seriously, and reserve the right to act upon it as per section 89 clause 5 of the Education and Inspections Act 2006. This means that the school reserves the right to deal with any bullying incident that pertains to the school "to such extent as is reasonable", whether it is on the school premises or in the online world. As there is no legal definition of bullying, for the purposes of this policy the school will use the following summary "the repeated use of electronic communication in any form, on any platform, which would cause harm or distress to another person."

4.2 The school will deal with any incidents on an individual case by case basis, using a set of sanctions that are proportionate to any behaviours demonstrated. The school will take into account:

- The context
- The intention
- The impact of any incident

4.3 before determining the response and actions to be taken. The school will allow a degree of flexibility in the application of actions e.g. a series of low level incidents would likely to be treated differentially from persistent and more serious incidents.

5. Internet Filtering

Monitoring

5.1 No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the Acceptable Use agreement. Monitoring will be carried out by the ESW IT Services Team or relevant ISP.

Audit / Reporting

5.2 Logs of filtering change controls and of filtering incidents will be made available to:

- Principals
- Online safety coordinator
- Online safety Director
- External Filtering provider / Local Authority / Police on request

5.3 The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

6. Safeguarding Monitoring (Securus)

Monitoring

6.1 Securus XT software offers a device level monitoring system that effectively captures online, off-line, typed and untyped activity. The system will monitor all activity on any device and will alert based on criteria that is maintained by Securus and updated daily. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the Acceptable Use agreement.

Alerting and Reporting

6.2 Activity that the monitoring software deems has met its criteria for an alert, is reviewed by the Securus FMS team. Their safeguarding trained team will assess the severity of an alert and will then contact nominated contacts within the school as appropriate. The team have access to the see the activity on the device before and after the alert which can be used to determine the context and rule out false positives.

7. Key steps in the process

Roles and responsibilities

7.1 Each school/establishment will need a named representative for the following posts, which will be recorded below:

- Safeguarding governor
- Safeguarding lead
- Child protection lead

7.2 Safeguarding governor

The elected online safety governor is responsible for holding their allocated school to account for effectiveness ofpolicy implementation. The elected governor is tasked with:

- Regular meetings with online safety lead and coordinator
- Overseeing safeguarding

7.3 The safeguarding lead is responsible for:

- Ensuring staff receive suitable training and development to enable them to carry out their online safety roles and train other colleagues, as relevant.
- Ensuring there is a system in place to monitor and support those who carry out the internal online safety monitoring role in school to provide a safety net.
- Updating the Senior Management Team (SMT) with regular monitoring reports
- Raising awareness of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.

- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitoring the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, governing body and other agencies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Meeting the online safety Lead & Governor to discuss current issues, review incident logs and filtering / change control logs when required.
- Reporting regularly to SMT.

7.4 Designated safeguarding lead / child protection lead

- The safeguarding and child protection leads should be aware of the potential for serious child protection/safeguarding issues to arise from:
- Sharing of personal data
- Access to illegal or inappropriate materials
- Inappropriate online contact with adults and strangers
- Potential or actual incidents of grooming
- Cyber-bullying

7.5 Senior Management Team (SMT)

The SMT is responsible for:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement
- Supporting the online safety (online safety) lead in the development of an online safety culture within the setting
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-

appropriate understanding of online safety and the associated risks and safe behaviours

- Making appropriate resources available to support the development of an online safety culture
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices
- To work with and support technical staff in monitoring the safety and security of school systems and networks
- To ensure that the designated safeguarding lead (DSL) works in partnership with the online safety lead

7.6 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current policies
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the online safety co-ordinator, Principal, ESW IT Services Manager for investigation, action or sanction
- digital communications with pupils should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils 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

7.7 ESW IT Services Team

The ESW IT Services Team are responsible for ensuring:

- that the ICT infrastructure is secure and is not open to misuse or malicious attack.
- that ESW meets the online safety technical requirements outlined in the Acceptable Use Policy.
- that users may only access the ESW networks through a properly enforced password protection policy, in which passwords are regularly changed.

- the appropriate ISP, Principal, IT Services manager is informed of issues relating to filtering.
- the filtering policy is applied and updated on a regular basis.
- The team keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal/ IT Services Manager for investigation / action / sanction.
- that monitoring software / systems are implemented and updated
- they report any breaches or concerns to the designated safeguarding lead and leadership team.

7.8 ESW Shared Services team

ESW Shared Services team are responsible for ensuring:

- They have an up to date awareness of online safety matters and of the current policies
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the online safety co-ordinator, Principal, ESW IT Services Manager for investigation, action or sanction
- They using the ICT systems in accordance with the Staff Acceptable Use Policy, which they will be expected to adhere/agree before being given access to school systems.
- Digital communications with pupils should be on a professional level and only carried out using official school systems

6.9 Pupils/pupils

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to adhere/agree before being given access to school systems.
- will be taught to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- will be taught 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 school policies on the use of BYOD. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school.
- be aware that this policy applies the trust's Online Safety Policy covers their actions out of school, if related to their membership of the school in line with section 89 clause 5 of the of the Inspections Act 2006 "to such extent as is reasonable"

6.10 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Schools within the Education South West will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing and accepting the Student Acceptable Use Policy
- Accessing the school website in accordance with the relevant school Acceptable Use Policy

6.11 Community Users

Community Users who access school ICT systems as part of the Extended School provision will be expected to sign/ acknowledge a Community User AUP before being provided with access to school systems.

6.12 Internet Filtering

The responsibility for the management of the trust's filtering policy will be held by the ESW IT Services Team. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems. All users have a responsibility to report immediately to the ESW IT Services Team any infringements of the trust's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

7. Procedures

7.1 Any concerns regarding the online conduct of any member of the school's community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as bullying, allegations against staff, behaviour and safeguarding/child protection.

7.2 Where staff are working directly with school social media schools within Education South West will safeguard members of staff working in these roles.

7.3 Internet Filtering

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged through the service desk system
- be reported to the Online Safety Group every term in the form of an audit of the change control logs

8. Local conditions statement

8.1 In some circumstances, local conditions mean that delivery will require local specific changes in the procedures. However, the core essence of the policy must be followed.

8.2 Please highlight below any school specific policy changes, this must be signed by the principal of the school and they're responsible for this change in policy guidelines.