The Stanway & Thomas Lord Audley Schools

E-Safety Policy

Last updated: January 2018

Contents:

Statement of intent

At The Stanway & Thomas Lord Audley Schools, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

The school is committed to providing a safe learning and teaching environment for all students and staff, and has implemented important controls to prevent any harmful risks.

e-Safety Officers:

The Stanway School	Mr Paul Child
The Thomas Lord Audley School	Mr Ross McKenzie

Designated Safeguarding Leads:

The Stanway School	Mr Chris Johnson
The Thomas Lord Audley School	Mrs Ann Bryant
e-Safety Governors	Mrs Nicola Elliott/Mrs Clancy Tassell

Signed by:

_____	Headteacher, Stanway	Date: _____
_____	Headteacher, Thomas Lord Audley	Date _____
_____	Chair of governors	Date: _____

1. Legal framework & Scope

1.1. This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997
- General Data Protection Regulation 2016

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Code of Conduct
- Cyber Bullying Policy
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Anti-Bullying Policy
- Child Protection Policy
- Behaviour Policy
- Staff Discipline & Dismissal Policy

2. Use of the internet

2.1. The school understands that using the internet is important when raising educational standards, promoting student achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all students, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard students.

3.3. The e-safety officer, is responsible for ensuring the day-to-day e-safety in the school, and managing any issues that may arise.

3.4. The e-safety officer is responsible for chairing the e-safety committee, which includes representatives of the school senior leadership team (SLT), teaching staff, governors, parents and wider school community.

3.5. The headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.6. The e-safety officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach students about online safety.

3.7. The headteacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.8. The e-safety officer will monitor the provision of e-safety in the school and each term will provide feedback to the headteacher and the Local Governing Board.

3.9. The e-safety officer will maintain a log of submitted e-safety reports and incidents.

3.10. The headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by students or staff.

3.11. The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.12. The e-safety officer will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

3.13. Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.

3.14. The governing body will receive a termly report from the e-safety officer. The e-safety officer will also attend at least one governors' meeting per year to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

3.15. The governing body will evaluate and review this E-Safety Policy on a termly basis, taking into account the latest developments in ICT and the feedback from staff/students.

3.16. The headteacher will review and amend this policy with the e-safety officer, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.17. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.18. All staff are responsible for ensuring they are up-to-date with current e-safety issues, including the E-Safety, Social Media and Anti-Bullying Policies.

3.19. All staff and students will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the headteacher.

3.20. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.21. The e-safety officer is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.22. All students are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

3.23. The ICT Manager will be responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- the school meets the e-safety technical requirements outlined in the ICT, Security and Acceptable Usage Policies.
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- he / she keeps 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
- the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator
- monitoring software / systems are implemented and updated as agreed in school policies

4. E-safety education

4.1. Educating students:

- Students will be taught about the importance of e-safety. This will ensure that they are aware of the safe use of new technology both inside and outside of the school.
- Students will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Students will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all IT suites and on the opening screen of student machines.
- Students are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate students about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold e-safety events, such as Safer Internet Week and Anti Bullying Week, to promote online safety. E-Safety assemblies will also be delivered when required. E-safety may also feature in our PSHE Enrichment Days.

4.2. Educating staff:

- A planned calendar programme of training opportunities is available to all staff members, including whole school activities and CPD training courses, which includes e-safety updates.
- All staff will undergo e-safety training updates on a regular basis, via staff meetings, briefings, to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy. E-safety advice/guidance is also available in the Code of Conduct.
- The e-safety officer will act as the first point of contact for staff requiring e-safety advice.

4.3. Educating parents:

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- Twilight courses and presentations will be run by the school for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

5.1. Internet access:

- Internet access will be authorised once parents and students have returned the signed consent form in line with our Acceptable Use Agreement.
- A record will be kept by the headteacher of all students who have been granted internet access.
- All users will be provided with usernames and passwords, and are advised to keep these confidential to avoid any other students using their login details.

- Students' passwords will be changed on a regular basis and their activity is continuously monitored by the e-safety officer.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor students' activity.
- Effective filtering systems will be established to eradicate any potential risks to students through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to students' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The schools' ICT Manager will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the e-safety officer.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Master users' passwords will be available to the headteacher for regular monitoring of activity.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the e-safety officer for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy. The headteacher will be consulted beforehand.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and prohibited from using any personal devices. This will be dealt with following the process outlined in section 7.4 of this policy.

5.2. Email:

- Students and staff will be given approved email accounts and are only able to use these accounts.
- The use of personal email accounts to send and receive personal data or information is prohibited.

- No sensitive personal data shall be sent to any other students, staff or third parties via email.
- Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages are not monitored.
- Any emails sent by students to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.3. Social networking:

- Use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.
- Students are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with students over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

5.4. Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or students will be published.

- Images and full names of students, or any content that may easily identify a student, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Students are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.5. Mobile devices and hand-held computers:

- The headteacher may authorise the use of mobile devices by a student where it is seen to be for safety or precautionary use.
- Students are not permitted to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during lesson time by students or members of staff for personal use.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the e-safety officer when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of students or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5.6. Network security:

- Network profiles for each student and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords will expire after 90 days to ensure maximum security for student and staff accounts.
- Passwords should be stored using non-reversible encryption.

5.7. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the ICT Manager.
- The e-safety officer will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.8. E-safety committee:

- The E-safety Policy will be monitored and evaluated by the school's e-safety committee on a termly basis.
- The committee will include a member of the SLT, the e-safety officer and the designated safeguarding lead (DSL), as well as a member of the governing body.

6. Cyber bullying

6.1. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

6.2. The school recognises that both staff and students may experience cyber bullying and will commit to preventing any instances that should occur.

6.3. The school will regularly educate staff, students and parents on the importance of staying safe online, as well as being considerate to what they post online.

6.4. Students will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.

6.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy and Cyber Bullying Policy.

6.7. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a student.

7. Reporting misuse

7.1. The school will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all students and staff members are aware of what behaviour is expected of them.

7.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to students as part of the curriculum in order to promote responsible internet use.

7.3. Misuse by students:

- Teachers have the power to discipline students who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Deputy Headteacher (Pastoral).
- Any student who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a student upon the misuse of the internet. This will be discussed with the Deputy Headteacher (Pastoral) and will be issued once the student is on the school premises.
- Complaints of a child protection nature, such as when a student is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection Policy.

7.4. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a Complaints Form.
- The headteacher will deal with such incidents in accordance with the Staff Discipline & Dismissal Policy and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

7.5. Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- If the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK, the police will be contacted

- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.

7.6. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the relevant school's e-safety officer or ICT Manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the SLT link manager for ICT who will liaise immediately with the ICT Manager.

7.7. e-Safety Incident Log

- Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.
- Using Smoothwall the designated IT services assistant will run a report under the following headings:
    - Abuse
    - Adult Content
    - Suicide
    - Radicalisation
    - Substance Abuse
    - Criminal Activity
    - Bullying
- The report will be generated on a daily basis.
- This report will be copied to:
    - SLT Link
    - E-Safety Officer
    - HoH & AHoH (who will record on SIMS Details and Actions)
- Incidents recorded on SIMS will fall under 3 headings:
    - Internal
    - External
    - E-Safety

8. Monitoring and review

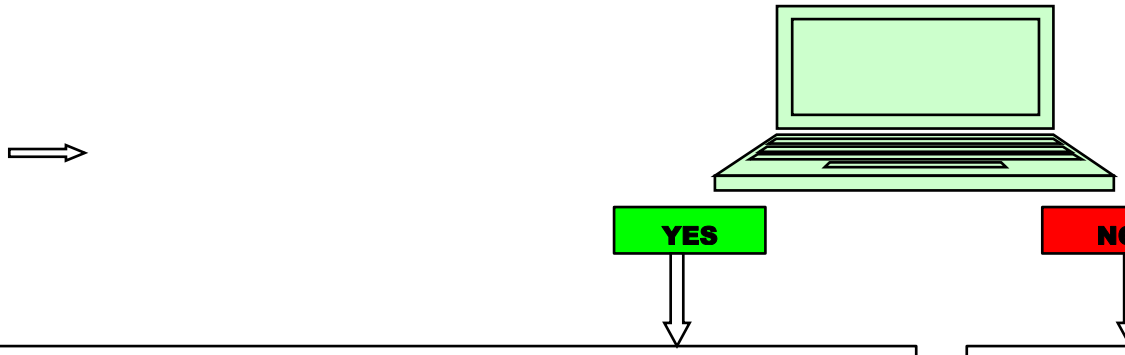
8.1. The e-safety committee will evaluate and review this E-Safety Policy on a termly basis, taking into account the school's e-safety calendar, the latest developments in ICT and the feedback from staff/students.

8.2. This policy will also be reviewed on an annual basis by the governing body; any changes made to this policy will be communicated to all members of staff.

8.3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

8.4. Staff and students will be involved in making/reviewing the Policy for ICT Acceptable Use through school council & staff meetings.

Essex flowchart to assist Headteachers, Senior Leaders and e-Safety Co-ordinators in the decision making process related to an <u>illegal</u> e-safety incident



- Inform Essex Police and Essex County Council
- Follow the advice given by the Police, or
- Confiscate the device and if related to the school network disable user account
- Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence
- If a student is involved contact Social Care Direct to make an emergency referral on 0845 603 7627
- If it involves a member of staff contact the LADO on 0330139797

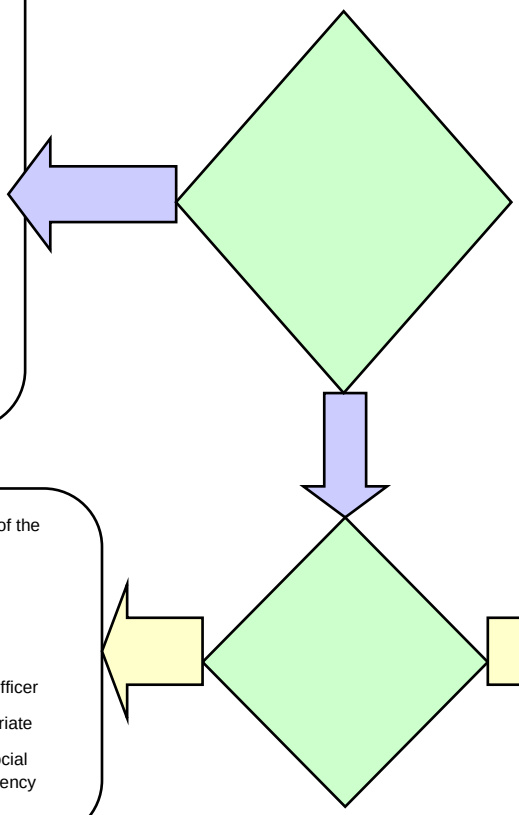
Go to next flowchart which outlines the process for non-illegal incidents

If a member of staff has:

- Behaved in a way that has, or may have, harmed a child
- Possibly committed a criminal offence
- Behaved towards a child in a way that indicates that s/he may be unsuitable to work with children
- Contact LADO on 0330139797
- Review evidence and determine whether the incident was accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate) and contact Schools HR on 03330139810 or your schools Link Officer

The Headteacher/e-Safety Co-ordinator should:

- **Record the incident in the e-safety log**
- **Keep any evidence**



Support the student by one or more of the following:

- Class Teacher
- e-Safety Coordinator
- Headteacher/Senior Leader
- Designated Child Protection Officer
- Inform Parent/carer as appropriate
- If the child is at risk contact Social Care Direct to make an emergency referral on 08456037627

- Review incident to decide if other students were involved
- Decide appropriate sanctions
- Inform Parent/Carer if serious or persistent incident
- If serious, consider informing the Duty Safeguarding Officer as the child instigator coold be at risk