STOUR VALLEY
COMMUNITY SCHOOL

E-Safety Policy

E-Safety Policy
Date approved: **February 2020**
Next review date: **February 2021**

1. Aims

ICT and the internet will be embraced as part of a world which students will need to be familiar with to conduct their lives within and beyond their educational years. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks, both in and out of school. It includes education for all members of the school community on risks and responsibilities and how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use.

2. Principles

School internet access will be designed for student use and will include filtering for all users. Students will be taught what internet use is acceptable and what is not and given clear guidelines for use. Staff should guide students through on-line activities that will support the learning outcomes planned for the students' age and maturity. The teaching and learning of e-Safety is embedded within the curriculum to ensure that the key safety messages about engaging with people are the same whether students are on or off line.

Information received via electronic communication requires good information handling skills as it may be difficult to determine origin and accuracy. In a perfect world, inappropriate material would not be visible to students using the internet, but this is not easy to achieve and cannot be guaranteed. Unfortunately students may, occasionally, be confronted with inappropriate material, despite all attempts at filtering and they will be given advice on how to deal with such situations in and out of school.

3. Responsibilities

Governors and Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-safety as part of the wider safeguarding across the School, with further responsibilities as follows:

- The Headteacher has designated an E-safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring e-safety is addressed in order to establish a safe ICT learning environment.
- Governors ensure e-safety is covered, within an awareness of safeguarding, and how it is being addressed within the school. They have the responsibility for ensuring that all safeguarding guidance and practices are embedded.
- The Local Governing Body takes responsibility for e-Safety and ensures the School has an Acceptable Use Policy (AUP) with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, and appropriate action is taken, which may include involving parents/carers, staff disciplinary measures or informing the police.

Designated E-Safety Lead

The designated e-Safety lead is Richard Lee.

It is the role of the designated e-Safety Lead to:

- Appreciate the importance of e-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their students and staff.

- Establish and maintain a safe ICT learning environment within the school, including that filtering and is set to the correct level and anti-virus software it up-to-date, and ensure that the AUP is reviewed annually.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, safeguarding and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Ensure there is transparent monitoring of the internet and online technologies along with a log of incidents to help inform future developments and safeguarding, where risks can be identified.
- Ensure that staff can check for viruses on electronic devices and transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised - Office 365 spam filter is in place, however 100% filtering cannot be guaranteed. Staff should refer to the Managing Allegations Procedure (Suffolk Safeguarding Children Board), for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged and should be avoided
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the SLT and offer advice as required.
- Make students aware that they cannot reset forgotten e-mail passwords. This has to be done by the e-mail administrator
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Students are taught what to do in the event of an incident.
- Promote the use of electronic communications in an appropriate way that does not breach the GDPR. All user are requested to remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Highlight the need for all personal storage devices which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the school development plan.
- Provide regular updates for students and staff on e-safety issues.

Students

Students will be:

- Expected to follow the Acceptable Use Agreement whilst within school as agreed on admission to the school. Breaching the Acceptable Use Policy may result in disciplinary action. Students are regularly reminded of the AUP and it is discussed in lessons.
- Taught to use the internet in a safe and responsible manner through Computing, PSHE, other curriculum areas as appropriate and extra-curricular activities.
- Encouraged to use appropriate language when emailing each other and staff members.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away.
- Expected to respect copyright and intellectual property rights and the correct use of published material.
- Mindful that the School Behaviour Policy states "All members of the school community have the right to feel safe. Any form of bullying is treated seriously and followed up as a matter of priority. Bullying is defined as "any physical, verbal or indirect abuse which is deliberately hurtful and causes distress, or which an

individual perceives to be bullying in nature". This includes cyber bullying."

4. Appropriate and Inappropriate Use of ICT

- Staff have a password to access a filtered internet service and know that this should not be disclosed to anyone or any device left unattended whilst logged in.
- All staff receive a copy of the Acceptable Use Policy which they need to sign and return to the School to be filed.
- If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report is made to the Headteacher immediately and then the Managing Allegations Procedure and the Safeguarding Policy will be followed to deal with any misconduct and all appropriate authorities contacted.
- The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
- File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the computer network.
- Should a student be found to misuse the online facilities whilst at school the consequence will be a ban from the network for an agreed period of time, with referral to the Designated Safeguarding Lead if necessary. Additional consequences will be in line with the school's Behaviour Policy.
- In the event that a student accidentally accesses inappropriate materials they should report this to an adult immediately and hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.
- Children will be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials as this may have legal implications.
- Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis. A firewall blocks certain network traffic or protocols based on rules set by Suffolk County broadband. Students and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school security controls (including internet filters, antivirus solutions or firewalls).

5. School E-mail Account

E-mail is an essential means of communication throughout the school community. Directed e-mail use can bring significant educational benefits to the learning environment. School e-mail accounts should not be considered private and the school reserves the right to monitor those accounts.

- All users are provided with an approved e-mail account within the school environment to able to understand different ways of communicating and using ICT to share and present information in different forms. Individual email accounts can be traced if there is an incident of misuse.
- Staff, Governors and students should use their school e-mail addresses for any school-based communication.
- If an offensive e-mail is received students must immediately inform their teacher; staff must inform the ICT Network Manager. Users must not send material or attachments by e-mail that the receiver may find offensive. Monitoring software is used to flag up inappropriate terms.
- Students are taught not to reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission from parents/carers.

6. Images

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

- Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that is an appropriate image for school.
- Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored centrally and not on personal devices, in line with safeguarding guidelines.
- Images of students will not be published on the school website without the permission of the parent/carer. Any student images or names will be checked to ensure they have the relevant permission for publication.
- Students will be advised about the reasons for caution in publishing personal information and images in social publishing sites.
- Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name.
- It is current practice by external media such as local and national newspapers to include the full names of students in their publications. Photographs of students should only be used after permission has been given by a parent/carer.

7. Social Networking and other Online Platforms

Social networking sites are used as a leading method of communication amongst both adults and young people. The service offers users both a public and private space through which they can engage with other online users. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with young people, there are a number of risks associated which must be addressed. With this in mind, both staff and students are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Instagram and Facebook).

In response to this issue the following measures are in place:

- Access to social networking sites is controlled through existing filtering systems. Access is not restricted as there is some legitimate use of social media, at which time access is controlled through the AUP.
- Students are advised against giving out personal details or information, which could identify them or their location (e.g. mobile phone number, home address, school/education setting or other establishment name, clubs attended, email addresses or full names of friends). Students are also warned about geo-location data used on smartphones.
- Students are discouraged from posting personal photos on social networking sites without considering how widely accessible the information is and the potential for misuse. Advice is also given regarding background images in photos, which could reveal personal details (e.g. house number, street name, school/education setting or other establishment uniform).
- Students are advised on social networking security and recommendations made for privacy settings to be activated for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- Students are taught about safe ways of using all aspects of the internet across the curriculum and specifically in Computing, PSHE and through assemblies.
- The curriculum makes students aware that social networking can be a vehicle for cyber bullying. Students are encouraged to report any incidents of bullying to the school allowing for the procedures, as set out in the Anti-bullying Policy, to be followed.

8. Social Networking Advice for Staff

Social networking outside of work hours, on non-school issued equipment is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with students such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles or viewing items such as personal photos.
- Staff should not engage in personal online contact with students outside of authorised systems and must not run social networking spaces for student use on a personal basis. However, professional use may be encouraged if specific to a dedicated learning outcome (eg. utilising social networking technology to provide additional support to students with their work).
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine to avoid fake profiles set up by students.
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a professional level.

9. Mobile Phones and Other Emerging Technologies

The use of mobile technologies can be used as an effective teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

- Inappropriate or bullying text messages.
- Images or video taken of adults or peers without permission being sought.
- Sexting - the sending of suggestive or sexually explicit personal images via mobile phones.
- Wireless Internet access, which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

Students are allowed to have mobile phones in their possession as long as they are turned off and stored securely out of sight. They may be used in lessons only with the explicit permission of a member of staff.

- Staff on visits will be issued with a school mobile phone, when contact with students or parents/carers may be required.
- If contact with students is necessary, staff must use school-owned equipment unless there is an emergency situation in which case a member of SLT should also be informed.
- The School is not responsible for any theft, loss or damage of any personal mobile device.

10. Protecting Personal Data

The quantity and variety of data held on students, families and staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The GDPR law gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. Personal data will be recorded, processed, transferred and made available according to GDPR.

11. Parents / Carers

- Each student receives a copy of the Acceptable Use Policy on admission to the School which needs to be read with the parent/carer, signed and returned to School confirming both an understanding and acceptance of the agreement.

- It is expected that parents/carers will explain and discuss the agreement with their child, so that the content is clearly understood and accepted.
- Parents'/carers' attention will be drawn to the school's E-safety Policy in the school prospectus and on the school website.

12. Managing Allegations against Adults Who Work With Children and Young People
Allegations made against a member of staff should be reported to the Designated Safeguarding Lead within the school immediately. In the event of an allegation being made against the Headteacher, the Chair of Governors should be notified immediately.

The Local Authority Designated Officer (LADO) is involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

13. CCTV
- CCTV is used within the school for monitoring purposes.
- All images recorded through the CCTV system are fully traceable with the date, time, and recording device.
- A system is in place to govern the day to day operation of the CCTV system. For data security purposes a restricted number of staff have access to any images and recordings held by the School. Staff with access to recordings are the Headteacher, Deputy Headteacher and Designated Safeguarding Lead and Network Manager.

14. Links to Other Policies
Please refer to the Behaviour and Anti-bullying Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs. The GDPR policy is displayed on the school website.

15. Monitoring and review
- The E-Safety Lead and Network Manager will monitor the use of online technologies by students and staff, on a regular basis.
- Staff should monitor the use of the internet during the school day.
- The Governing Body will be responsible for monitoring the effectiveness of this policy and reviewing it annually. Any changes will be made in line with legislation.

Ratified by Governing Body	
Date	