

SHERBORNE AREA SCHOOLS' TRUST



E-Safety Policy

Published:	Oct 2021
Review due:	Oct 2024
Author:	SAST Governance

SAST Document Control Table			
Document Title		SAST E-Safety Policy	
Author (Name & Job Title)		SAST	
Version No.		1.0	
Date Approved		15.10.21	
Approved By		BB	
Date of Next Review		Oct 2024	
Document History			
Version	Date	Author	Notes of Revisions

SAST E-Safety Policy

1. Introduction and Scope

This policy applies to all members of Sherborne Area Schools' Trust "SAST", including all staff, student/pupils, volunteers, parents/carers, visitors and community users who have access to or are users of SAST digital technology systems, both in and out of any school within the trust.

E-Safety encompasses any electronic device that is capable of recording, storing, transferring or publishing digital media. It includes, but is not limited to, mobile phones, laptop computers, desktop computers, tablet PC, media recorders, MP3 players and game consoles as well as other collaboration tools and personal publishing tools. This policy highlights the need to educate students about the benefits and risks of using technology and provides safeguards and an awareness for users to enable them to control their online experience in a safe and meaningful way.

Internet and associated technologies are an excellent tool and resource to enrich learning, however SAST recognises that there are still dangers related to their use, especially in relation to young students. Some examples of this are:

- Bullying via chat or email
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

The Education Act 2011 empowers Headteachers to, such extent as is reasonable, 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 including searching for and confiscation of harmful equipment or devices. This is pertinent to incidents of online-bullying or other E-Safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. Any disciplinary sanctions imposed by staff can only be carried out in accordance with the published School Behaviour for Learning policy.

SAST has a duty of care alongside that of parents and other members of the community, to protect its pupils and students from the dangers of associated with using unfiltered online resources, and this can be achieved by many different mechanisms working together. The purpose of this E-safety policy is to outline the measures the trust takes to ensure that students can work in a safe environment and that any E-safety issue is detected and dealt with in a timely and appropriate fashion.

SAST's E-safety policy should be read in conjunction with other policies including, but not limited to the; **ICT Acceptable Use, Behaviour for Learning Principles, Anti-Bullying, Curriculum, Child Protection and Safeguarding, Social Media, Data Protection and Information Security policies**. This policy supplements all other legislation applicable to schools including the Prevent Duty as outlined in the Counter-Terrorism and Security Act 2015.

2. Roles and Responsibilities:

The following section outlines the online safety roles and responsibilities of individuals and groups within SAST.

2.1 Trust Board

Trust Board members are responsible for the approval of and compliance with this E-Safety Policy and for reviewing the effectiveness of the policy with support from the SAST Executive staff. The approval of this policy can be delegated to SAST executive staff with permission from the Trust Board. Regular monitoring of the effective implementation of this policy is delegated to local governors of schools under the SAST Scheme of Delegation.

2.2 Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety may be delegated to another member of the SLT. 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 online safety allegation being made against a member of staff (see flowchart at Appendix A with regard to dealing with online safety incidents). The Headteacher / Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. The SAST Head of IT and Infrastructure will ensure that there are technical solutions in place to allow for ongoing monitoring online safety with the Trust network.

2.3 Head of IT and Infrastructure, Network Manager / Technical staff

The IT Support Team are responsible for ensuring:

- That schools' technical infrastructures are secure and not open to misuse or malicious attack
- The school meets required online safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy
- The filtering policy 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 online safety technical information in order to effectively carry out their online safety role and to inform, share and update others as relevant
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse/attempted misuse can be reported to the Trust Executive team or Headteacher for investigation / action / sanctions

2.4 All staff (Teaching and non-teaching)

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of this E-Safety Policy and practices
- They have read, understood and signed the Staff ICT Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Headteacher or Senior Member of Staff for investigation / action / sanction

- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems and in accordance with data protection law
- Ensure that online safety issues are embedded in all aspects of the curriculum and other activities, and to remind students at every possible opportunity when their work involves the use of ICT
- Students / pupils understand and follow this E-Policy and Student ICT Acceptable Use policies
- Students / pupils 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.
- Where available, staff MUST use monitoring software when in IT rooms to ensure students are on task and not at risk.
- 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.
- Ensuring that where sound and video media that is based on streaming services, its use is pre-planned and that the whole material has been checked as being suitable for the age of the students that are accessing the material.

2.5 Designated Safeguarding Lead or Designated Persons

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
- Online-bullying

2.6 Students / Pupils

- Are responsible for using the school digital technology systems in accordance with the Student ICT Acceptable Use Agreement
- 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 and use of images and on online-bullying.
- Should understand the importance of adopting good online 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

2.7 Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Schools will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, and information about national or local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online 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 and on-line pupil records
- Their children's personal devices in the school

Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through a range of activities, including but not limited to:

- Curriculum activities
- Letters, newsletters, website and online learning platform notices
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant E-Safety awareness websites and publications
- Sharing material that has been distributed via the Trust that has been designated as needing to be shared with parents and carers.

2.8 Governors, Volunteers and Community Users

Non-staff users who access school systems as part of the wider school provision will be expected to sign an ICT Acceptable User Policy as part of their induction. Community users will accept that no alteration can be made to existing systems that would potentially reduce the effectiveness of security systems in place in the school or that may introduce vulnerabilities that could be exploited.

3. Education (See DFE Non-Statutory Guidance: [Teaching Online Safety in School](#))

Why Internet use is important -

The Internet is an essential element in 21st century life for education, business and social interaction. Each school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the curriculum and a necessary tool for staff and pupils. Students use the Internet widely outside school on a range of devices and it is important that they learn how to evaluate Internet sources, identify potentially harmful situations and to take care of their own safety and security. Internet use will enhance learning. The Internet access provided by the Trust has been tailored expressly for pupil and staff use and will include appropriate filtering. It is important to bear in mind that with the ever-changing nature of the Internet the filtering provided by the Trust cannot be guaranteed to be 100% effective and all adults should be continually aware of the need to be vigilant when students are using technologies to access on-line materials. Students should be taught what Internet use is acceptable and what is not and given clear objectives for Internet use when it is being used in lessons. To this end all Internet access will be planned to enrich and extend learning

activities. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the Students' age and maturity. Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, and staff will make use of any technologies in place to monitor and restrict access to Internet resources so that its use is focused and controlled.

3.1 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work, regardless of their age.

3.2 How will pupils learn to use ICT appropriately?

If students are to be as safe at home as they are at school, they need to recognise the risks for themselves. Each school will have a programme of teaching appropriate skills in the early years which will reinforce the safe and appropriate use of the Internet. These skills will be revisited by staff when they use ICT to support the teaching and learning. It is the responsibility of ALL staff to ensure that any use of ICT by students is appropriate. The understanding of appropriateness will be further developed through the PSHE/learning for life curriculum and assemblies which should further develop the students understanding of the risks and opportunities of using the Internet, and social networking sites.

3.3 Pupil Responsibility

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and digital literacy is therefore an essential part of the school's online safety provision. All schools will have a program of study embedded into their curriculum that will allow all pupils to understand the dangers and opportunities on online usage. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum (and not the sole responsibility of those teaching IT) and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on- line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the ICT Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites that have been checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Below Key Stage 4, it is not good practice to simply allow students to “search the Internet” for resources without supervision. By the time pupils have reached Key Stage 4, they should be competent to undertake research that is safe. Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3.4 Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training may be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This should be regularly updated and reinforced. An audit of the online safety training needs of all staff will be held centrally by SAST.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and ICT Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

3.5 Training – Trustees and Local Governors

Trust Board members and Local Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any subcommittee or group involved in technology and online safety, health and safety or safeguarding. Part of their monitoring role may include reviewing:

- Levels of Internet Access
- Information system security
- The capacity and security of the ICT systems provided by the Trust
- Cybersecurity measures including virus protection

- Where computers have access to sensitive financial data over the Internet, additional security software installed to protect the finances of the Trust.
- Incident reporting

3.6 E-mail

All emails sent from the ICT systems within the Trust to external bodies will encompass a standard footer statement.

- Students, staff, governors and volunteers may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher and staff should advise their line manager or IT support if they receive an offensive or inappropriate e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation by pupils should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Where e-mails are inadvertently sent to the wrong recipient or personal data (including email addresses) are sent using the To or CC field rather than the BCC field, these incidents must be reported immediately as a data breach to the trust Data Protection Officer (dpo@sast.org.uk)

Where necessary a whole-class or group e-mail address should be used at Key Stage 2 and below;

Access in school to external personal e-mail accounts may be blocked. This is because it will not be secure and conform to the relevant legislation governing security of data.

Emails are scanned and some emails may be quarantined as the software may suspect the content or the attachment. The IT teams can release these emails BUT only after action has been taken to prove the identity of the sender. This is best achieved by contacting the sender, explaining the email has been automatically quarantined, and asking for it to be sent again. This will prove that the email is not a spoofed email. If it is quarantined again IT will know it is legitimate and release it.

No one should open any attachment or follow any link within an email if they do not recognise the sender. The best advice is if the user is unsure, delete the email and contact IT Support.

3.7 Published content and the school website

- The contact details on the individual school websites will be the school address, e-mail and telephone number.
- Staff or students' personal information will not be published except staff names at the discretion of the Headteacher.
- Each school should designate a person with overall editorial responsibility and ensure that content on the school's website is accurate and appropriate.

3.8 Publishing pupil's images and work (See also **SAST Data Protection Policy**)

- Consent from Students/Pupils over 12 and from parents of pupils under 12 is sought at the beginning of each year from parents or carers before photographs of students can be used on the school website;
- Photographs that include students who have given permission will be selected carefully and will not enable individual students who have not given permission for use to be identified. These will be vetted by a member of the leadership team in relation to consent under Data Protection law;
- Student's full names will not be used anywhere on any website or Blog, particularly in association with photographs except with explicit permission;
- Each school will record on the MIS system all parents who have not specifically consented to their children's pictures being used in publicity;
- Student work can only be published with the permission of the student.
- Staff should refer to the **SAST Data Protection Policy** before using any pupil images internally or externally.

3.9 Managing filtering

Filtering is used across SAST to protect children and staff. The trust uses RM filtering and Lightspeed filtering in school.

The recommendation is that filtering should not be an in-house solution. Where new schools join SAST, they are given period of grace until their existing support contracts expire, and the expectation is that they then move to the current Cloud based supported SAST solution, usually a managed service provided by a 3rd party. Having an externally provided solution will allow for continuity of service in the event of technicians moving on from their current role.

- The SAST solution should allow for the ability to filter by user, user type, group and device used.
- Where the Trust oversees the filtering, it will ensure that the systems in place to protect students are reviewed and improved on an annual basis as necessary;
- The Trust will proactively add inappropriate websites to the filter lists as appropriate. Unblocking may only be permitted once the site has been discussed with a senior member of staff and this authorisation then communicated in writing to the technical team. Users need to be aware that this process is not immediate and it is recommended that at least 2 days notice is given of any change request to be processed.
- If staff or students discover an unsuitable site, it must be reported to a member of teaching staff or the ICT support teams who will then take the appropriate action. In certain circumstances they may filter the site immediately until a review of the site can be undertaken;
- ICT Support staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- Any material that the school believes is illegal will be reported to IT Support and the Headteacher in the first instance. Should it be necessary, this will then be passed to the relevant authorities.

3.10 Managing Online Video Communication including Remote Learning

- See **SAST Staff and Student ICT Acceptable Use Policies**.

3.11 Managing Emerging Technologies

Technologies are continually changing and emerging. Whilst it is not possible to cover all such devices, it is intended that the policies of the Trust have been written in such a way that they cover newest technologies. This policy, along with the **SAST ICT Acceptable Use Policy** and **Staff Code of Conduct Policy** also cover the use of mobile phones whilst on any trip organized by the school. Students need to be aware that the sending of abusive or inappropriate text messages is forbidden and will be dealt with under the guidance of the individual schools Behaviour for Learning Policy.

Staff will be usually issued with a school mobile phone where contact with pupils is required for example on foreign trips or outward-bound activities. Staff should not issue their personal phone numbers to students. The use of portable media devices is acceptable so long as use is appropriate. Wireless access points have been provided by SAST in each school to encourage the students to use them to support their studies. The Internet access afforded through these devices is via the normal filtered Internet Access.

3.12 Protecting Personal Data

See **SAST Data Protection Policy**.

3.13 Cloud Storage

SAST staff must note that:

Not all cloud- based storage technologies are safe and secure. The Trust follows the guidance provided by the DFE and at the time of review, the only recognised cloud storage permissible by the staff in the Trust are Google Drive and Microsoft One drive as provided by SAST.

Staff should not store any other data related to their day-to-day work in any other cloud-based systems without first discussing this with the Head of IT and Infrastructure.

3.14 Social Media Applications

See also **SAST Staff Code of Conduct Policy** and **SAST Social Networking Policy** in relation to personal social media accounts and the management of school-based social media accounts.

When official school / academy social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under the **Staff Code of Conduct Policy** and school **Behaviour for Learning** policies.

3.15 Abuse of Mobile Devices and Media within and Outside School

The schools within the Trust will take a serious and robust approach to any misuse of technology which occurs on any site. If the abuse is via a mobile phone, the phone will immediately be confiscated and an investigation undertaken by a member of the pastoral care team or Headteacher. If the issue relates to inappropriate images, then the Designated Safeguarding Lead must be immediately informed. In these circumstances staff must not under any circumstances view the images or forward them onto another person as this is an offence in its own right.

- Parents/guardians will be informed about the incident and any resulting actions taken as punishment;
- Where necessary, external agencies will be informed including the Police;
- All such incidents will be logged on the individual school's My Concern safeguarding reporting system.

3.16 Bring Your Own Device (BYOD)

See **Staff/Student ICT Acceptable Use Policies**.

Appendix A – Flowchart for dealing with an Online/E-Safety Incident

