SOUTHERN ACADEMY TRUST

E-safety Policy

<table>
<tr><th colspan="4">Document Control Table</th></tr>
<tr><td colspan="2"><b>Document Title</b></td><td colspan="2">E-safety Policy</td></tr>
<tr><td colspan="2"><b>Author and Job Title</b></td><td colspan="2">Adam Tuffin - IT Systems Manager</td></tr>
<tr><td colspan="2"><b>Version Number</b></td><td colspan="2">V1</td></tr>
<tr><td colspan="2"><b>Date Approved</b></td><td colspan="2">09/12/2019</td></tr>
<tr><td colspan="2"><b>Approved by</b></td><td colspan="2">Board of Trustees</td></tr>
<tr><td colspan="2"><b>Date of Review</b></td><td colspan="2">01/09/2020</td></tr>
<tr><td colspan="4"><b>Document History</b></td></tr>
<tr><td><b>Version</b></td><td><b>Date</b></td><td><b>Author</b></td><td><b>Note of Revisions</b></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Contents

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, career.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents.

Safeguarding is a serious matter; at Southern Academy Trust (SAT) we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the SAT website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use and Internet Policy (Both available as online declarations). At secondary a copy of the Students Acceptable Use and Internet Policy is in the students' planner and at the beginning of each school year must be signed by both student and parent. With the signed declaration page in the planner and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Review Date: Sept 2019 Next Review: Sept 2020

Policy Governance (Roles & Responsibilities)

Governing Body

The governing bodies' of each school are accountable for ensuring that the schools has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within their school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- A governor will have overall responsibility for the governance of e-safety at their school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within their school. The day-to-day management of this will be delegated to a member of staff.

The Headteacher will ensure that:

- E-Safety training throughout their school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety member of staff (referred to as the e-Safety Coordinator) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Coordinator

The e-Safety coordinator will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher and IT System Manager.
- Advise the Headteacher, IT Systems Manager, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behavior management software) are fit for purpose through liaison with the Trust IT Department.

- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

Trust IT Department

The Trust IT Department are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety coordinator and Headteacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of their Headteacher.
- Any e-safety incident is reported to the e-Safety Coordinator (and an e-Safety Incident report is made in SIMS), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the e-Safety Coordinator or the Headteacher to decide.
- Attend E-safety Training/CPD
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

- The boundaries of use of ICT equipment and services in each school are given in the student Acceptable Use and Internet Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behavior policy.

- e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Careers

- Parents play the most important role in the development of their children. The school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered – these will be available via the Trust website.

- Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. At secondary parents will sign the student Acceptable Use and Internet Policy before any access can be granted to school ICT equipment or services.

Technology

SAT uses a range of devices including PC's, laptops, Apple Macs and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – We use 'Lightspeed' software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT/e-Safety co-ordinator and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – We use Office 365's spam filters and conditional rules that helps prevent any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message, email attachments containing executable files.

Office 365 Conditional Access – We use Multi Factor Authentication for all users who wish to access Office 365 outside of the schools. This is to help prevent phishing email scams from executing successfully.

Security Policy – Applies to mobile devices. This enables mobile devices force the user to put a passcode on their device and also stops any unauthorised user accessing the system. Username and passwords are required to access email on a mobile device.

Passwords – All staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The Trust IT Department will be responsible for ensuring that passwords are changed.

Anti-Virus – The anti-virus software used in school is called 'ESET'. All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. Trust IT Department will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use and Internet Policy; Parents and students upon signing in the planner their acceptance of the Acceptable Use and Internet Policy (Secondary School only).

Office 365 – All staff are reminded that emails, MS Teams & SharePoint conversations are subject to Freedom of Information requests, and as such the Office 365 is to be used for professional work-based communications only.

Students are permitted to use the school Office 365 system, and as such will be given their own email address. Primary student accounts have external incoming emails blocked. The email address will be made up of their year of joining in their school and their surname and first three letters of firstname. 12Smithjoh@shaftesburyschool.co.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Radicalisation/Online Safety– All staff ensure that children are safe from terrorist and extremist material when accessing the internet in schools. SAT ensures that suitable filtering is in place.

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself. By cyber-bullying, we mean bullying by electronic media such as:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, SnapChat, Youtube and Ratemyteacher etc.

LEGAL ISSUES

Cyber-bullying is generally criminal in character. There are laws that apply to cyberspace.
SAT trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. SAT endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems. Where appropriate and responsible, SAT audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, SAT reserves the right to take action against those who take part in cyber-bullying.

- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.
- SAT supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.
- SAT will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school.
- SAT will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware they have a duty to bring to the attention of the Head any example of cyber-bullying or harassment that they know about or suspect.

Continued online safety is delivered through lessons, assemblies.

Social Networking – there are many social networking services available; SAT is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within SAT and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the safety coordinator who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in schools.
- Twitter – used by the schools as a broadcast service (see below).
- Facebook – used by the schools as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety coordinator, DPO, Trust IT Department or in his/her absence the Headteacher. The e-Safety coordinator/DPO will assist you in taking the appropriate action to deal with the incident and to fill out an incident log. This is done through SIMS.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, SAT will have access to material informing them of safety issues which is suitable to the audience.

E-Safety for students is embedded into the Digital Literacy curriculum in KS3, through Tutor sessions, assemblies and drop days; whenever ICT is used in the schools, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety coordinator is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Acceptable use and Internet Policy

The staff Policy is available as an online secure document on the trust intranet pages. Staff are to read and accept the policy. This is then recorded and managed by the DPO.