Stephen Sutton
Multi-Academy Trust

E-Safety Policy

This policy applies across all partner schools in the Stephen Sutton Multi-Academy Trust (SSMAT). It is available on the SSMAT website and is accessible from our schools' websites.

POLICY APPROVAL and REVIEW

Review date: ***Nov. '20***

Approval needed by: ***Trust Board***

Adopted: ***Sep. '18***

Next review date: ***Sep. '22***

1. Introduction / Overview

1.1 New technologies are integral to people’s lives. The internet and other digital technologies create extraordinary opportunities for learning and communication. In a school context, therefore, it is appropriate that students are able to take advantage of information and communications technology and that they are taught how to use it appropriately and effectively in a safe and supportive environment.

1.2 This E-Safety Policy is concerned with the duty of care that the Stephen Sutton Multi-Academy Trust (SSMAT) and its partner schools have for its students, with regard to the risks to their safety and wellbeing that the internet and other technologies can present. However, the policy also addresses the appropriate use of the internet and associated technologies by staff, volunteers, visitors, governors and directors, who are expected to meet professional standards of conduct and whose actions contribute very significantly to the context in which students’ safety is protected.

1.3 The dangers presented by inappropriate use of the internet and other technologies, both inside and outside school, include:

- access to illegal, harmful or otherwise inappropriate images and other content;
- unauthorised access, by others, to personal information;
- the risk of ‘grooming’ by adults who make contact through social networking [see also the Trust’s Safeguarding Policy];
- sharing, and subsequent distribution, of personal images (including images of an intimate / sexual nature);
- cyber-bullying;
- online gambling;
- plagiarism and copyright infringement;
- illegal downloading of audio/video files;
- the indiscriminate use of information found on the internet, without considering the reliability and credibility of the sources; and
- The potential for excessive use (including addiction to online gaming), with a negative impact on social and emotional development and on academic outcomes.

1.4 It is impossible to eliminate the risks presented by the internet and associated technologies. However, through good education and through the provision of opportunities for students to use technology responsibly, with guidance and, as required, consequences, students can develop the judgement, confidence, resourcefulness and resilience to understand the risks and make good decisions in an increasingly complex world.

2. Roles and responsibilities

2.1 Trust Board

The Trust Board is responsible for the Trust's E-Safety Policy, ensuring that this creates an appropriate framework for keeping members of the school community safe and ensuring legal compliance.

2.2 Local Governing Body (LGB)

The LGB of each of the Trust's partner schools is responsible for the school's procedures and programmes that operationalise the Trust E-Safety Policy and for reviewing the effectiveness of the school's implementation of the policy and procedures. Each LGB has a 'Governor with Responsibility for Safeguarding' and this person, as part of their remit, checks compliance with the Designated Safeguarding Lead (DSL) and other colleagues, as nominated by the Head of School / DSL. In particular, the Designated Governor should check e-safety filtering methodologies and logs of e-safety incidents.

2.3 Head of School

The Head of School is responsible for ensuring the safety (including e-safety) of members of the school community and for ensuring that colleagues are appropriately trained to be able to fulfil their responsibilities effectively. The Head of School must also ensure that there are appropriate ICT network filtering systems in place. Where misuse is reported, the Head of School (or delegated senior member of staff) is responsible for ensuring that this is investigated and an appropriate course of action is taken, including disciplinary sanctions. Furthermore, consistent with their broader safeguarding responsibilities, the Head of School is specifically responsible for the management of allegations, in relation to e-safety, that are made about a member of staff. [Consistent with broader safeguarding procedure, an allegation relating to e-safety about the conduct of the Head of School should be referred to the Chair of Governors or the Executive Headteacher of the Trust].

2.4 E-Safety Officer / Designated Safeguarding Lead (DSL)

Within each partner school, it should be clear which person takes the E-Safety Officer role. SSMAT believes that, in most cases this role is best played by the Designated

Safeguarding Lead, who is highly trained in understanding the risks that young people face and the procedures that ought to be followed for all safeguarding concerns. It is likely, in most contexts, this person will need to work closely with another member of staff who has a stronger knowledge of the school's ICT network and how the school's filtering system operates. Nevertheless, the safeguarding expertise is the most important criterion for selecting an e-safety officer. Furthermore, by accommodating this role within the broader safeguarding role, it is less likely that there will be duplication of effort and inconsistency in procedures and communications.

2.5 Network Manager

The school's Network Manager (or, equivalently, the most senior person with responsibility for the school's ICT infrastructure) is responsible for ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack. Furthermore, they must ensure that users may only access the school's ICT network through a properly enforced password protection procedure, through which passwords are regularly changed. This person also ensures that the school's filtering and monitoring procedures are applied and updated on a regular basis and that system use is monitored carefully, with logs kept and incidents reported to senior staff.

Where a partner school has a managed ICT service that is provided by an external contractor, the Head of School must ensure that the service provider carries out all of the e-safety measures that would otherwise be done by the school, as set out in this E-Safety Policy. The service provider must also be aware of the Safeguarding Policy and the Acceptable Use Agreement.

2.6 Colleagues

Colleagues are responsible for ensuring that:

- they have read and understood the Trust's E-Safety Policy and their school's related procedures and guidance;

- they have read, understood and signed the school's Acceptable Use Agreement (AUA);

- they report and suspected misuse, problem or concern relate to e-safety to the E-Safety Officer (as explained above, this should be the DSL unless specifically stated otherwise);

- any digital communication with students takes place on a professional basis, using school ICT systems [Personal contact details must not be given to students];

- (as appropriate to their role) they take opportunities to discuss e-safety issues, where relevant to curriculum activities;
- they help students to understand and follow the school's e-safety procedures;

- (as appropriate to their role) they help students to understand the basic of good research skills, the need to avoid plagiarism and the ned to uphold copyright regulations;

- monitor directly the use of ICT in lessons and other extended learning / extra-curricular activities;

- they are aware of e-safety issues related to the use of mobile devices (including phones and cameras) and that they ensure that, as appropriate, they are used responsibly in a way that is consistent with policy and procedure; and

- (as appropriate to their role) where internet access is used in lessons, where practicable, sites are checked prior to student use and correct procedures are followed for dealing with a situation where unsuitable material is found in internet searches.

2.7 Students

Students are responsible for using ICT in accordance with the Acceptable User Agreement form (which they will need to sign in order to gain access to school ICT systems) [At Key Stage 1, parents/carers sign on behalf of their children]

They are also encouraged to report abuse, misuse or access to inappropriate sites and the level of expectation that they do so is proportional to their age, maturity and level of understanding.

Students should also develop an understanding of good e-safety practice (including the use of mobile phones) and understand that the E-Safety Policy (including, in particular, cyber-bullying and other inappropriate use of social networking) covers their actions off the school site, as well as on it, where the activity related to their membership of eth school.

2.8 Parents and carers

Parents and carers play an important role in helping their children to understand the need to use the internet, and associated technologies, responsibly. However, some parents and carers will need support and information to enable them to exercise this responsibly effectively, as they will often be less experienced ICT users than their children. The school therefore has a role to play in helping parents to understand these issues through information sessions, letters home and website updates.

Parents and carers are specifically responsible for signing (endorsing) the school's Acceptable Use Agreement form.

2.9 Community users

Any members of the community must sign an Acceptable Use Agreement form, in order to gain access to the school's ICT network.

3. Curriculum

3.1 The internet is now an integral part of modern life, including education, business and social interaction. Schools ought therefore to provide suitable access, where practicable, to the internet to support learning. In order to achieve this the following measures are taken:

- the school's network infrastructure, including filtering systems, are designed with the specific purpose of enabling internet access that supports students' learning;
- students are given clear objectives relating to internet use, outlining what is (and what is not) acceptable;
- where students need to research topics that may result in internet searches being blocked (e.g. racism, drugs, discrimination), colleagues can request that access is made available, for a temporary period, by requesting that the Network Manager, 'whitelists' those sites from the filtered list for the period of study [All requests of this nature must be logged in an auditable manner, noting the reasons for access];
- students are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation; and
- students have digital literacy units in the curriculum that focus on staying safe online, including how to use a search engine, digital footprints and cyber-bullying.

3.2 These issues are addressed, in a planned way, through the taught ICT/Computing and Personal, Social, Health and Enterprise (PSHE) curricula, through taught lessons and through the assembly/tutorial programme.

4. Training

4.1 Colleagues

In order to observe and implement the E-Safety Policy and related school procedures effectively, staff need to be trained and their knowledge needs to be updated on a regular basis. This is done through:

- key e-safety messages and information included in the induction programme for new staff;
- e-safety training needs audited annually and programmed through the school's training plan;
- ensuring the E-Safety Officer / Designated Safeguarding Lead (DSD), Network Manager and, as appropriate, Head of Schooland other nominated staff, receive external training and updates, appropriate to their roles, on a regular basis; and
- ensuring that colleagues receive updates from lead staff (as above) and are clear on which colleagues hold the positions of responsibility referred to in the E-Safety Policy.

4.2 Governors and directors

Governors and Trust directors receive updates from the Head of School and Executive Headteacher / Trust Business Manager (respectively) and the LGB's Governor for Safeguarding also gets briefed on a regular basis by the school's E-Safety Officer / DSL and shares this knowledge with the LGB. Periodically, or as required, Trust-level training is also organised for governors and directors, to enable them to conduct their role from an informed and objective position.

5. Social networking

5.1 Social networking sites (e.g. Facebook and Twitter) provide the facility to chat and exchange information and images online. The online environment is very different to the experience of communicating face to face and actions are often taken that are ill judged, sometimes with serious consequences. For this reason, the following measures are taken:

- social networking sites are blocked using the school's filtering system. [Where a member of staff needs temporary access to a social networking site for educational reasons or to investigate a concern that has been reported, authorisation is needed from a senior member of staff and the usage, with the reason provided, must be logged by the Network Manager];

- students are advised to interact only with known friends and family on social networking sites and to deny access to others;

- students are taught about the risks of disclosing personal details about themselves and the school they attend and the risks associated with the use of photos and videos over social networking sites;

- staff are also advised to ensure that they have appropriate controls in place (‘private’ settings) to restrict access to their social networking pages / sites [Students must not be listed as approved contacts];

- colleagues are also advised that any comments that they make through social networking that identify them as a member of the school and are deemed inappropriate may be subject to disciplinary action;

- colleagues are further advised that any abusive or threatening remarks mane about a member of the school community and any remarks made about the school or the Trust, that are deemed defamatory, may also be subject to disciplinary action; and

- parents are also advised that the school / Trust will consider taking legal action, where a parent makes abusive or threatening comments towards members of the school community or makes derogatory, defamatory comments about the school or the Trust.

6. Potential radicalisation and the ‘Prevent’ duty

6.1 The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. SSMAT schools ensure that suitable filtering is in place to prevent access to inappropriate content and students are taught how to stay safe, in relation to potential radicalisation, when using the internet and social networking.

6.2 As with other online risks of harm, every member of staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups. This is addressed through the schools’ induction and training programmes.

6.3 Parents are also provided with information about e-safety that include a focus on potential radicalisation.

6.4 See the Trust’s ‘Promoting British Values and Preventing Radicalisation and Extremism’ Policy and the ‘Safeguarding Policy’ for further detail.

7. Mobile phones, cameras and other mobile digital devices

7.1 The Head of School uses their judgement, in relation to the context in which they work and the age and maturity of the students in their school, regarding the school's position in relation to bringing mobile digital devices on to the school site and regarding their use around the school and in classrooms. School expectations and procedures in relation to this issue must be documented and clearly communicated to all members of the school community and, as appropriate, visitors to the school. [In an Early Years setting, there is a statutory safeguarding requirement to have a clear policy that mitigates against misuse of mobile devices to capture images / videos of young children for personal use or distribution and protects staff against potential allegations]

7.2 Unless it is required in an emergency, colleagues must not use personal mobile phone numbers / email accounts to contact parents or students. In the unusual situation where this is / has been necessary, they should inform the Head of School of the circumstances at their earliest opportunity.

7.3 Mobile devices (phones, tablets, iPads etc.) must be password protected and kept securely to prevent unauthorised use.

7.4 In accordance with data protection and human rights legislation, partner schools have their own 'Use of Photographic Images Policy'. Common principles across SSMAT include:

- where parents/carers, for whatever reason, do not want images of their children to appear in the press, on the website on in other public contexts, then their wishes will be observed;

- where the Head of School, or a nominated member of staff, gives permission for photos and videos to be taken of their own children in school events, they must clarify that they must not share the images on social networking sites, or otherwise distribute them, if other students appear in the background [In some circumstances, e.g. a swimming gala, it would not be sensible to permit photographs / videos to be taken at all]; and

- colleagues should use school phones/cameras/iPads to capture images, rather than their own personal devices.

8. Responding to e-safety incidents and concerns

8.1 Consistent with broader safeguarding procedures, an allegation about the online activity of a member of staff should be reported to the Head of School. Where the allegation is about the Head of School, the matter should be referred to the Chair of Governors or Executive Headteacher.

8.2 The Designated Safeguarding Lead (DSL) (or, in their absence, the Designated Safeguarding Deputy (DSD)) should be informed of any online safety concern. The DSL will then escalate the matter, as appropriate. For more information, please consult the Trust's Safeguarding Policy.

8.3 Cyber-bullying, along with any other form of bullying is not tolerated. For further details on the school's approach, please consult the school's Ani-Bullying Policy and its Behaviour Policy. Common principles across SSMAT schools include:

- all incidents of cyber-bullying are recorded, together with any evidence that is collected;

- all reported incidents and allegations are investigated, with support provided for those affected;

- where a criminal offence may have been committed, then the DSL and/or Head of School will liaise with parents/carers and consider the appropriate involvement of the police;

- parents/carers and students are advised to keep (e.g. 'screenshot') any evidence on online bullying;

- in order to investigate a reported case of cyberbullying, school ICT system activity logs are examined, witnesses /interested parties are interviewed, and the service provider is contacted (as appropriate);

- appropriately assertive disciplinary sanctions are used, in accordance with the school's Behaviour Policy; and

- the DSL deals with and, as appropriate, escalates any safeguarding issues that become apparent, or are suspected. See the Trust's Safeguarding Policy for further detail.

Stuart Jones; Nov. '20