KINGSTONE ACADEMY TRUST

APPROVED POLICY DOCUMENT

E- Safety Policy	
Relevant School/s:	**KHS and KTPS**
Policy Officer:	**Sally Spreckley**
Approval:	**Delegated**
Date of Review:	**October 2018**
Next Review:	**3 years or upon legislative change**
Distribution:	**Public, on website**

1. Introduction

E-Safety is essentially about creating a safe environment when using ICT; this includes the use of the internet and social networking sites. One of the key risks of using the internet, email or instant messaging services is that young people may be exposed to inappropriate material.

This policy is intended to outline the Academy's approach to preventing online safeguarding issues, including cyber bullying and sexting, as well as detailing how we respond to e-safety issues when they emerge. This may be exposure to material that is pornographic, hateful or violent in nature; that encourages activities that are dangerous or illegal; or that is just age inappropriate or biased.

2. Definition

This policy is closely related to the guidance contained in:

- Keeping Children Safe In Education – statutory guidance to schools and colleges (DfE September 2018)
- The Prevent Duty – departmental advice for schools and childcare providers with regard to Radicalisation via the internet and social media (DfE June 2015)

This policy should be read alongside the:

- KAT Safeguarding Policy
- Behaviour and Anti-Bullying Policy
- Staff Code of Conduct
- Whistleblowing Policy

3. Aims

Our aim is to provide clear guidelines and information to students, their parents and staff about how to keep young people safe and by dealing rapidly with any emerging concerns through a consistent approach. This will involve close communication with parents and where necessary, liaison with Children's Services, the Police and other relevant agencies.

Education is the key to minimising the online risks to students. Responsible use of the internet, including social networking will be discussed through PSHE lessons, assemblies and form time sessions are used regularly to educate students on appropriate online behaviour covering use in school and outside of school.

3.1 E- Safety

- The Academy will work in partnership with parents, the DfE, the Police and the Network Service Provider to ensure systems to protect students are reviewed and improved
- The Network Manager will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable.
- If filtered websites need to be used by staff, they must inform the Network Manager to have them unblocked for a set period of time
- The Academy may invite external agencies such as the Police to support our e-safety programme, as a way of educating young people further about risk. For child perpetrators, this may involve work which focuses on respecting themselves and others.
- The Academy will address the following:
    - cyber bullying and sexting, with specific reference to our Anti Bullying Policy;

• the safe use of social media, including utilising privacy settings and the pitfalls of sharing personal information and photographs;
• the significance and consequences of their online behaviour, including digital footprints, legal sanctions and career prospects;
• online stranger danger, including how to recognise and report suspicious activity;

- Advice and guidance will be sought from The Child Exploitation and Online Protection Centre (CEOP, http://www.ceop.police.uk/) which brings together law enforcement officers and specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse.
- Information will be provided to parents and carers via the school website which will address safety issues associated with social media and online communities. These articles outline the measures parents can take to educate and protect their children at home as well as informing them of the Academy's approach in terms of prevention and response to concerns.
- An e-safety audit will be carried out regularly. (see Appendix 1)

3.2 Guided Educational Use

- The curriculum requires students to learn how to locate, retrieve and exchange information using ICT.
- Curriculum internet use will be planned, task orientated and educational within a regulated and managed environment.
- Students will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Students will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Any user discovering unsuitable sites must report the address and content to a teacher or the Designated Child Protection Officer as appropriate

3.3 Internet Access

- The Academy will maintain an up to date record of all staff and students who are granted Internet access
- All Internet access is monitored and recorded using electronic means
- Inappropriate use of the Internet will be dealt with in accordance with the Academy's Behaviour Policy
- Pupils may only use approved email accounts on the Academy system
- Access in Academy to external personal email accounts will be blocked for all students
- Pupils must immediately tell a teacher if they receive offensive email
- Pupils must not reveal details such as address/telephone number of themselves or others or arrange to meet anyone in email communication
- Email sent to an external organisation should be carefully written and authorised by a teacher before sending
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

3.3 Academy Website Content

- The point of contact on the website will be the Academy address, email and telephone number. Staff and students' home information will not be published.

- Use of photographs showing students and students' names will not be used on the website without parental consent (KAT is GDPR compliant)
- The copyright of all material will be held by the Academy or be attributed to the owner where permission to reproduce has been obtained

3.4 Social Media

- Students will not be allowed access to public or unregulated chat rooms, social networking sites and forums
- Students may only use regulated sites – this use will be supervised whenever possible, and the importance of safety will be emphasised

3.5 Mobile Phones

- Mobile phones are not permitted to be seen in school during the school day unless directed by a member of staff (ref. School Rules)

4. Responsibilities

4.1 All Stakeholders

It is the responsibility of all members of our school community, including teaching and non-teaching staff, governors, volunteers and students, to prevent and tackle e-safety issues. In line with the KAT Safeguarding Policy, all e-safety concerns should be shared at the earliest opportunity with the DSL or Deputy DSL and in any case before the end of the school day.

- Students will be instructed in responsible and safe internet use before being granted access
- Staff training in safe and responsible internet use and on the contents of this policy will be provided as required
- A partnership approach with parents will be encouraged, with relevant information on issues covered by this policy made available
- Cases of internet misuse and other disciplinary breaches related to the policy will be dealt with through the Academy's Behaviour for Learning Policy, and Safeguarding Policy, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel (after consultation with HSCB and Police)
- Any complaints associated with the application of this policy will be dealt with through the Academy's Complaints Procedure

4.2 The Executive Headteacher

It is the responsibility of the Executive Headteacher to ensure that e-safety concerns are monitored and that staff remain appropriately trained to respond to such concerns. It is also the responsibility of the Executive Headteacher to ensure that preventative work is ongoing with students and that awareness raising among parents is ongoing.

4.3 The Designated Safeguarding Lead (DSL)

- The DSL is responsible for ensuring that technical staff are aware of what constitutes an e-safety concern which it would be necessary to report.
- The DSL will report regularly to the safeguarding governor on incidents of e-safety concerns and the subsequent actions and outcomes within the Academy.
- Breaches to our Academy network protocols will be dealt with rapidly by our network manager in liaison, where appropriate, with the DSL and/or other relevant pastoral leaders.

- Where the Academy receives information of a safeguarding nature concerning online activity which has taken place outside school, the Academy is equally committed to engaging with the students concerned and their parents to resolve the situation.
- Where we feel there is an ongoing risk to a young person, Children's Services and occasionally the Police, may be contacted to provide further support.
- Where it is felt that an ongoing risk is not a concern, the Academy is likely, usually following advice from Children's Services, to deal with the issues directly with students and their parents. This may involve meetings with students and parents whereby boundaries/ restrictions to internet access may be imposed.

4.4 Staff

All staff are made aware that it is a breach of our Code of Conduct to have students as 'friends' on social media and that students and staff members should not communicate via personal telephone or email accounts. Staff are also made aware that their online posts which may bring the Academy into disrepute are not acceptable under the Staff Code of Conduct. which informs all staff of our expectations in terms of protecting their identity and upholding an online presence that is appropriate to their professional position.

5. Review

- Methods to identify, assess and minimise risk will be reviewed regularly
- The Academy's ICT systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly
- Files held on the Academy's network will be regularly checked
- Use of portable media such as memory sticks and CD will be reviewed regularly
- Downloading of unauthorised files will be prohibited, and where possible blocked

Appendix 1 KAT e-Safety Audit

Completed by:	**Date:**			
Policy	Yes	Partly	No	**Evidence and Comments**
The Academy has a set of policies which cover the following: Online Safety; Mobile phones; Use of Images; Social media; Bullying.				E safety Policy Safeguarding Policy School Rules Behaviour Policy
All policies are easily accessible to staff, pupils and parents.				Website and shared area
The online safeguarding policies have been adapted to incorporate the specific needs and requirements of the Academy.				
The policies have been reviewed and approved by SLT and the Governing Body.				Minutes
There is a nominated member of the Governing Body who has strategic oversight of online safety.				Safeguarding Governor
Online safety policies are updated regularly to reflect changes in technology and national guidance *(at least annually).* Policies are also revisited following online safety incidents, to implement any lessons learnt.				On-going monitoring required
The Academy has a clear "Acceptable Use Policy" which outlines expectations for staff, parents, pupils and visitors regarding the use of technology in the Academy.				Visitor Policy Staff Code of Conduct
There are effective sanctions in place for anyone breaching the Academy's policies.				
The Academy regularly monitors and evaluates online safety approaches and mechanisms to ensure that the policy is consistently applied.				Alongside annual review of safeguarding policy

Responding to incidents	Yes	Partly	No	Evidence and Comments
Online safety is clearly identified as a safeguarding issue and concerns are managed in the same manner as other safeguarding issues.				
The DSL takes primary responsibility for online safety concerns that occur in the school.				
There are clear reporting mechanisms for pupils, parents/carers and staff, who have online safeguarding concerns.				Pastoral system Safegusding concern reporting sheets
There are specific procedures for responding to incidents of peer-on-peer abuse, including; Youth Produced Sexual Imagery (sexting) and cyber-bullying; in accordance with expectations in Keeping Children Safe in Education 2018.				Safeguarding Policy
All members of the community are aware of the process for reporting concerns; all online safety incidents are passed to the DSL and/or Headteacher *(in cases of allegations against staff)*.				
There are well developed strategies in place to ensure pupils feel safe and confident to report concerns, such as telling an adult if something online makes them feel worried, upset or uncomfortable.				
Online safety incidents are recorded and monitored by the DSL.				
Appropriate steps are taken to identify and protect vulnerable members of the community such as: looked after children, pupils with special educational needs or disabilities.				
All members of the wider community are aware of the				

process for reporting escalating concerns externally; all staff understand the Academy's whistleblowing procedure if they feel their concerns are not being managed appropriately.				

Infrastructure	Yes	Partly	No	**Evidence and Comments**
Access to the internet and Academy's network is secure.				
The Academy uses an appropriate internet service provider and implements appropriate filtering and monitoring.				
The use of Academy owned devices is monitored and there are robust procedures in place for responding to any concerns that are identified, in accordance with KCSIE 2018 and Prevent Duty.				
Personal data is managed securely online, in accordance with the statutory requirements of the GDPR 2018. All staff have due regard for data protection and understand the impact of data security. *E.g. Written parental consent for photos, encrypted emails, etc.*				
The Academy provides dedicated devices for taking photographs and making/receiving business communications *e.g. emails, phone calls, etc.*				
Members of staff do not use personal devices for business related activity. Emails, calls and other business related activity *(such as official social networking)* is done using the Academy's dedicated devices.				
All technology, apps and devices are subject to strict risk assessments prior to being introduced to pupils.				

Photographs or videos taken by the Academy are only shared in accordance with the Academy's Image Use Policy.				

Education and Training	Yes	Partly	No	Evidence and Comments
All members of staff *(including support staff)* receive regular and up-to-date online safety training. *(This is either stand-alone or incorporated within general safeguarding training).*				
The DSL has attended appropriate online safety/safeguarding training to ensure they have a higher level of knowledge regarding online safety issues.				
Members of staff receive regular updates regarding changes to policy and guidance or emerging online safety concerns.				
Staff induction training includes explicit reference to online safety, with regards to professional conduct and online reputation.				Code of Conduct
Staff role-model positive behaviours online by maintaining clear professional boundaries with parents and pupils. *I.e. keeping social network accounts private and not accepting pupils/parents as 'friends'.*				Code of Conduct
Pupils receive age appropriate, progressive and embedded online safety education throughout the curriculum.				
Pupils who are considered to be at increased risk online (such as children in care, children with SEND, children experiencing loss or trauma or children with mental health concerns) are provided with targeted or differentiated online safety education.				Informally as identified consider methods of differentiating.

The Academy has considered a range of strategies to support pupils in developing their own understanding of online safety and how to keep themselves and others safe. *For example, peer education.*				
The Academy engages with local and national events to promote positive online behaviour, e.g. Safer internet day and Anti-bullying week.				Needs to be embedded in the calendar
The Academy actively works to engage parents in their children's online safety education and signposts to support outside the Academy.				Opportunity for more to be put in place.
The Academy website includes online safety advice for pupils and parents and links to other organisations. There are also links to relevant online safeguarding policies and contact details of the DSL.				
The Academy offers training and support for parents and carers to ensure they understand online safety risks and their roles in safeguarding their children at home.				

Action Plan				
Key area for development		Resources, support or activity required	Date Completed	Signed
1				
2				
3				
4				
5				
6				