KEN STIMPSON COMMUNITY SCHOOL

e-Safety Policy

2015

1. Introduction.

We believe that all individuals within the school community have the right to develop their learning, skills and knowledge in a safe, secure and supportive environment, free from intimidation, prejudice or discrimination of any kind, and they should be guided to extend this beyond school into the wider community. This extends to interactions online and through technology, rather than limiting to face-to-face communication. E-Safety is described as the school's ability to protect and educate students and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate. This is carried out through:

- Teaching, modelling and promoting respect and tolerance for each other online, on social networks and through other technology
- Helping everyone towards an understanding of what is right and wrong
- Supporting everyone in forming good relationships online
- Helping those who have been perpetrators of cyber bullying or exhibited cyber bullying behaviour as well as their victims to develop positive strategies to cope with negative emotions and stress.

This e-safety policy was approved by the *Governing Body on:*	***June 2015***
The implementation of this e-safety policy will be monitored by the:	*ICT Across the Curriculum Coordinator, Child Protection Officer, Leadership Team*
Monitoring will take place at regular intervals:	*Termly*
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*May 2017*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Parents/Carers, LA Safeguarding Officer, Police*

2. Why is an e-Safety Policy necessary?

2.1 The school believes that its students have the right to use technology in a supportive, caring and safe environment without the fear of being bullied. All institutions, both large and small, contain some numbers of students with the potential for exhibiting bullying/inappropriate behaviour. If a school is well disciplined and organised, it can minimise the occurrence of internet/technology abuse. The school also has a clear policy on the promotion of good citizenship, where it is made clear that cyber bullying/online abuse is a form of anti-social behaviour and will not be tolerated. A preventative approach to cyber bullying and the importance of respecting others online is also taught in ICT, Computing, tutor time and assemblies and is promoted across all aspects of school life.

There are three main areas of risk;

2.1.1 Content: being exposed to illegal, inappropriate or harmful material

2.1.2 Contact: being subjected to harmful online interaction with other users.

2.1.3 Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

2.2 It is important, therefore, that the school has a clear written policy to promote this belief, where both students and parents/carers are fully aware that any e-safety complaints will be dealt with firmly, fairly and promptly. In some instances of misuse the school may feel it necessary to involve the police. The school will work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school.

3. Education

3.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision.

3.2 e-safety should be a focus across areas of the curriculum and staff should reinforce e-safety messages to students. e-safety is planned and delivered as part of the Computing and PSHE curriculums, along with tutor time activities and assemblies focusing on increasing awareness of issues relating to this area. The school promotes initiatives such as **Get Safe Online Week** and **Safer Internet Day** through pastoral, PSHE activities and Computing lessons.

3.3 Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an important part in the education of their children. The school aims to support parents/carers with this by sharing curriculum activities and updates, articles in school newsletters, magazines and pages on the VLE. An e-safety publication for parents has been produced and actively shared with parents of children at the school and those of prospective parents in the local area.

3.4 e-safety training is provided for staff across the school. The Child Protection Officer conducts formal training regularly and is supported by the e-safety ICT Across the Curriculum Coordinator and IT Technicians. Governors are invited to attend these training sessions as deemed appropriate.

4. Communications

4.1 The school allows students to use a range of technology, including mobile phones and tablets, at agreed periods in the school day. Mobile phones are permitted at break and lunch time (social times) but not in lessons unless deemed appropriate by the class teacher and relevant to their learning.

4.2 The table below outlines the agreed acceptable use of communication technology in school.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓					✓		
Use of mobile phones in lessons		✓	✓	?			✓	
Use of mobile phones in social time	✓				✓			
Taking photos on mobile phones / cameras		✓		?			✓	
Use of other mobile devices e.g. tablets, gaming devices		✓					✓	
Use of personal email addresses in school, or on school network	✓						✓	
Use of school email for personal emails				✓			✓	
Use of messaging apps		✓				✓		
Use of social media		✓				✓		
Use of blogs	✓					✓		

Key: ✓ Definite Action
? Possible Actions

5. Social Media and Professional Identity

5.1 School staff undertake training including acceptable use of social media, potential risks and ensuring security settings are in place. Staff are encouraged to avoid engaging on social media with students, except for the IT Technicians through the school social media accounts for informative purposes. Staff are aware of e-safety and what it means to them as professionals.
School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

6. Unsuitable/inappropriate activities

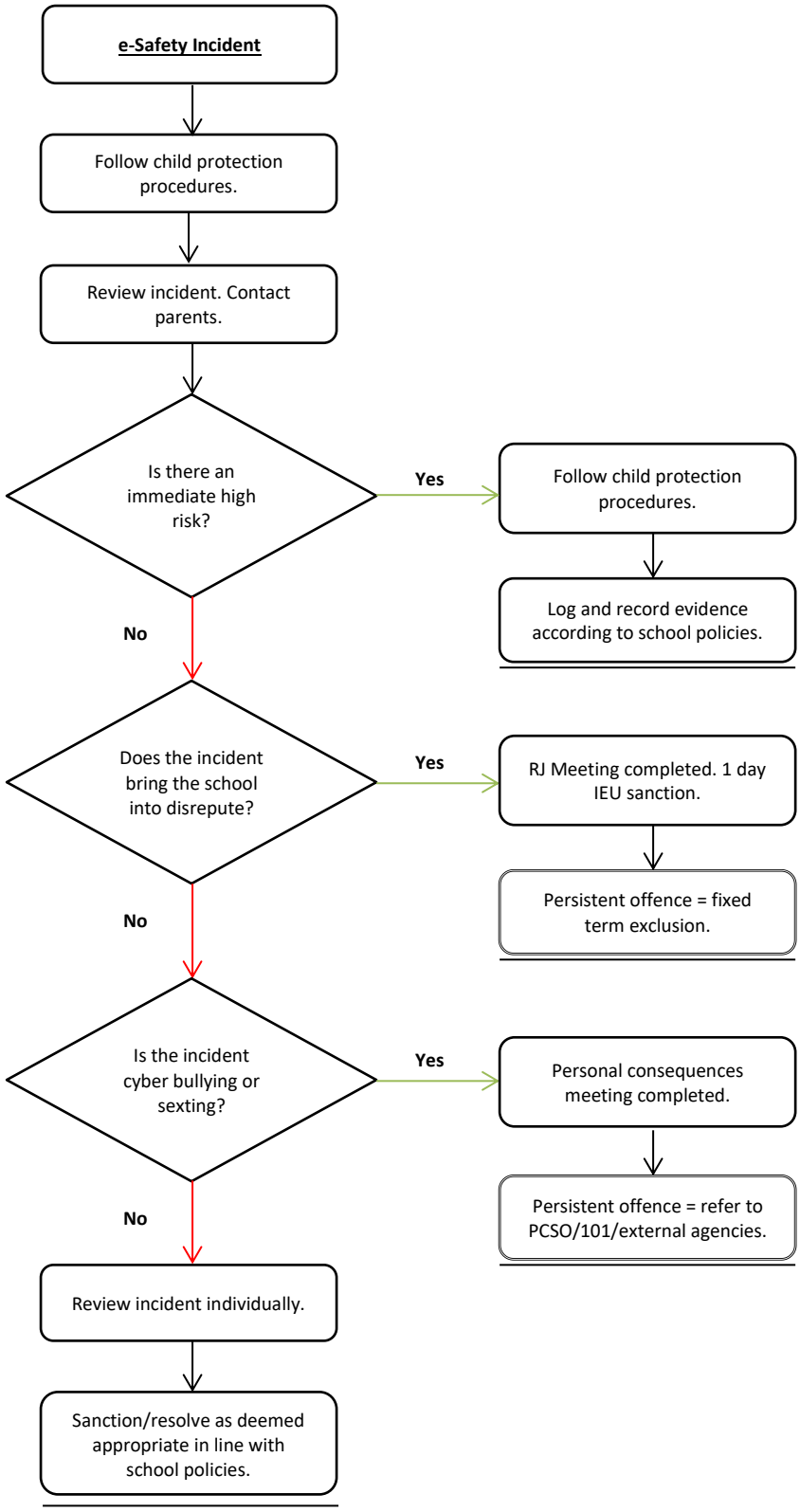
6.1 The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
	Pornography					✓
	Promotion of any kind of discrimination					✓
	Threatening behaviour, including promotion of physical violence or mental harm					✓

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	
Infringing Copyright					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✓	
On-line gambling						✓
On-line shopping / commerce				✓		
File sharing			✓			
Use of social media			✓			
Use of messaging apps					✓	
Use of video broadcasting e.g. YouTube			✓			

7. Response to Incidents

7.1 The flow chart below details the processes followed when responding to an e-Safety incident. External agencies are included where appropriate.



7.2 The table below indicates the sanctions for students if an incident occurs.

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Faculty / Head of House	Refer to Principal/SLT	Refer to Police/PCSO	Refer to technical support /ban	Inform parents / carers	Removal of network / internet access rights	Warning issued	Further sanction e.g. detention / exclusion	Confiscation
Deliberately accessing or trying to access material that could be considered illegal		✓		✓						
Unauthorised use of non-educational sites during lessons	✓	✓			✓					
Unauthorised use of mobile phone / digital camera / other mobile device	✓	✓				✓				
Unauthorised downloading or uploading of files	✓	✓			✓		?	✓		
Allowing others to access school network by sharing username and passwords		✓			✓	✓		✓		
Attempting to access or accessing the school network, using another student's account		✓			✓	✓		✓	✓	
Attempting to access or accessing the school network, using the account of a member of staff		✓			✓	✓			✓	
Corrupting or destroying the data of other users		✓			✓	✓			✓	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓		✓			✓	
Continued infringements of the above, following previous warnings or sanctions		✓	✓	?		✓			✓	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓	?		✓			✓	
Using proxy sites or other means to overthrow the school's filtering system		✓		?	✓	✓			✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓				✓	✓		✓		
Deliberately accessing or trying to access offensive or pornographic material		✓		✓	✓	✓			✓	
Receipt or transmission of material that infringes the copyright of another person or the Data Protection Act	✓				✓	✓		✓	✓	

Key: ✓ Definite Action
? Possible Actions

7.3 The paragraph below indicates the possible sanctions for staff if an incident occurs.

Staff are personally responsible for what they communicate in social media and must bear in mind that what is published might be read by member of the school community including, staff, parents, pupils, the general public, future employers and other professionals. Staff must ensure that their online profiles are consistent with the professional image expected by school and should not post material which damages the reputation of Ken Stimpson Community School, others, or which causes concern about their suitability to work with children and young people. Those who post material which may be considered inappropriate could render themselves vulnerable to criticism or allegations of misconduct which may be dealt with under the school's disciplinary procedure.

Remember social media is not a private means of communication and it can be accessed by people you are unware have association within the professional network in which you work within. If in doubt do not post it.

8. **Filtering of Content**

8.1 The responsibility for the management of the school's filtering policy will be held by the Technical Services Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

9. **Recording**

9.1 All incidents **MUST** be recorded and Heads of House and Senior Leadership Team will receive regular communication to ensure the safety of students.

Parents who have reported an incident or concern will be contacted to discuss their concerns.

Policy Reviewed by Paul Swift & Lee Chambers – January 2017

Changes to document:

- Change of job title from ‘Senior IT Technician’ to ‘Technical Services Manager’