Warden Park
'The Best From All'

SUSSEX LEARNING TRUST

E-safety

Type: Trust Policy
Status: Statutory
Application: All Member Academies
Review Date: April 2017

Issue Status:-

Date	Version	Comment	Committee	Owner
1st April 2015	1	Original document	SS	CG

Electronic copies of this document are available to download from: T/drive

Author:		
Updated/Reviewed by:		
Due for Ratification:	Secondary Standards Committee	
Ratified:	P Bradbury (Chair)	Date

Available publicly on Website: Yes
Electronic copies of this document are available to download from: T/drive

E-Safety Policy

Scope of the Policy

This policy applies to all members of the Trusts community (including staff, students, volunteers, parents / carers, visitors etc.) who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy.

The Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Co-ordinator.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with Trust's Digital Services Team staff .
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reports regularly to Senior Leadership Team

Director of Digital Services & Network Team:

- Ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Ensure that the school meets the e-safety technical requirements outlined in national E-Safety Policy and guidance.
- Ensure that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- Keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- Makes sure that the use of the *network, Virtual Learning Environment (VLE), remote access, email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator for investigation / action / sanction.*

Teaching and Support Staff:

- Ensure they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- Ensure they have read and understood the school Acceptable Use Agreement (AUG).
- Make sure they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction.
- Ensure that digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.
- Ensure that they are not 'friends' with students on social-networking sites and take every reasonable precaution to ensure that students cannot access personal content posted by them online.
- Ensure that e-safety issues are embedded in all aspects of the curriculum and other school activities.
- Ensure that students understand and follow the school e-safety and Acceptable User Agreement.
- Monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, tablet computers, cameras and other hand-held devices and that they monitor their use and implement current school policies with regard to these devices.

Child Protection Liaison Officer:

- Should be trained in e-safety issues and be aware of the potential for serious child Protection issues to arise from:
    - Sharing personal data
    - Access to illegal/inappropriate materials

- Inappropriate on-line contact with adults/stranger incidents of grooming
- Potential or actual
- Cyber-bullying
-

Students / pupils:

- Are responsible for using the school ICT systems in accordance with the Student 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 school policies on the use of mobile phones, tablet computers, digital cameras and other hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-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.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, letters and the website.

Parents and carers will be responsible for:

- Endorsing the Student ICT Acceptable Use Agreement on entry to trusts schools
- Accessing the school website / VLE / online student records in accordance with the relevant school Acceptable Use Policy.
- Understanding the importance of talking to their child about their online profiles regularly (your child should be happy to show you their online profiles) and taking all reasonable precautions to ensure that their child/children are using the ICT Resources available to them at home safely.
- Reporting to the school any incidents that they become aware of (relating to their child or another child) that have occurred during school time so that they can be dealt with quickly.
- Dealing with incidents that arise outside of school time.

Education of Students

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. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / Learning for Life/ other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Education of Parents/Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The trust will therefore seek to provide information and awareness to parents and carers through:

- Letters & the school website
- Parents evenings

Education & Training of Staff

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

- E-Safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required.

Training of Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered through participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by the Digital Services Team who will keep an up to date record of users and their usernames. Users will be required to change their password periodically.

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Digital Services staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Digital Services.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand-held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- Where students are allowed to freely search the internet and/or use tablet computers, staff should be vigilant in monitoring the content of the websites the young people visit and the applications they are using.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Use of digital and video images - Photographic, Video

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students				
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	X				X			
Use of mobile phones in lessons		X				X		
Use of mobile phones in social time	X				X			
Taking photos on mobile phones / cameras		X					X	
Use of other mobile devices eg tablets, gaming devices		X				X		
Use of personal email addresses in school, or on school network		X					X	
Use of school email for personal emails	X				X			
Use of messaging apps		X					X	
Use of social media		X					X	
Use of blogs		X					X	

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to their form tutor or Head of Year, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

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. (This list is should not be treated as exhaustive or definitive it is for guidance only). The school policy restricts certain internet 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					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
File sharing		X				
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting eg Youtube			X			

Responding to incidents of misuse:

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The E-Safety Coordinator and Headteacher should be informed immediately so that they can respond immediately.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows: (This list is should not be treated as exhaustive or definitive it is for guidance only).

Staff

Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X			X		X
Unauthorised downloading or uploading of files	X	X	X			X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X	X		X	X	X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X			X		
Deliberate actions to breach data protection or network security rules	X	X	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X		X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X			X		X
Actions which could compromise the staff member's professional standing	X	X	X			X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X	X			X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X			X	X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X

Students / Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X					X	X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X						X	
Unauthorised use of social media / messaging apps / personal email	X	X						X	
Unauthorised downloading or uploading of files	X	X			X			X	
Allowing others to access school / academy network by sharing username and passwords	X	X			X	X		X	X
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X	X	X	X	X		X	X
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users	X	X				X		X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X			X	X		X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X				X		X	X

Review: April 2017