POLICY DOCUMENT

Policy Title	E-Safety POLICY
Policy Reference	**SUAS.**

DISCLOSABLE UNDER FREEDOM OF INFORMATION ACT 2000	Yes / No	Yes
TO BE PUBLISHED ON WEBSITE	Yes / No	Yes

POLICY OWNERSHIP	
Governor Committee:	Pastoral
Department responsible:	Pastoral
Post-holder: *(Title and Name)*	Mrs K Berwick – Deputy Headteacher
LINKED PROCEDURES REF:	
Responsible Person - Procedures	

POLICY IMPLEMENTATION DATE:	July 2017
PLANNED REVIEW INTERVAL:	1 year
PLANNED NEXT REVIEW DATE:	July 2018

Stratford-upon-Avon School welcomes comments and suggestions from the public and staff about the contents and implementation of this policy. Please write to the Compliance Manager at the school address or email your comment to policy@stratfordschool.co.uk.

POLICY OUTLINE

Roles and responsibilities of staff members and nominated individuals in relation to E-Safety. Identifies the policy, monitoring procedure & actions to be taken by staff members.

PURPOSE

To implement robust E-Safety procedures and polies as part of the school's commitment to safeguarding.

IMPLICATIONS OF POLICY

Procedures to be followed by staff members and nominated individuals in relation to E-Safety.

EQUALITY ANALYSIS

Every policy will be subject to an Equality Analysis (EA) completed by the policy writer, which should be circulated to all those being consulted, with the draft policy.

CONSULTATION

Consultation will be with all staff, prior to presentation for approval by the Governing Body (Pastoral Committee).

PROCEDURE

Procedure is the method by which the strategic intent of the policy is realised, and is thus an 'instruction manual' on how the policy outcome is to be achieved.
The procedure which supports this policy is within this document and therefor will be subject to review by the Pastoral Committee and Governing Body.

RELATED POLICIES AND PROCEDURES

- *Child Protection and Safeguarding Policy*
- *Data Protection Policy*
- *Behaviour Policy*
- *Photographic Images of Students Policy*
- *Whistle Blowing Policy*

DOCUMENT HISTORY

The policy will be subject to regular review once ratified by the Governing Body.
The history of the policy will be recorded using the chart following:

Date	***Author /Reviewer***	***Amendment(s)***	***Approval/ adoption date***
June 2017	*K.Berwick*	*Created policy*	*TBC (July 2017)*

Development / Monitoring / Review of this Policy
This e-safety policy has been developed by following the SWGfL template and will be reviewed by the Governors and Designated Safeguarding Lead (DSL) before publication.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Monitoring of student behaviour data
- Monitoring of green forms / safeguarding issues

Scope of the Policy
This policy applies to all members of the school (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both on and off site.

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, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school 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 e-safety roles and responsibilities of individuals and groups within the school

Governors / Board of Directors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents. A member of the Governing Body / Board has taken on the role of Safeguarding Governor. The role of the Safeguarding Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- reporting to relevant Governors / Board / committee / meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care 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 DSL.
- The Headteacher and (at least) another member of the Senior Leadership Team (SLT) 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.
- The Headteacher / DSL are responsible for ensuring that they and other relevant staff receive suitable training 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.

Designated Safeguarding Lead (DSL):

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- 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 / relevant body
- liaises with school technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with the Safeguarding Governor to discuss current issues
- reports regularly to Senior Leadership Team

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they 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
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / DSL / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem: In the case of staff, to the Headteacher for investigation / action / sanction. In the case of a student, a green form is completed
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other relevant activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand 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 and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records
- their children's personal devices in the school

Policy Statements

Education – 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of Computing / SPHERE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students will 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.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters & web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day

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.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews of the safety and security of school academy technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the network manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical 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 technical incident / security breach to the relevant person, as agreed). Staff concerns reported to the head, student concerns recorded on a green form.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.

Bring Your Own Device (BYOD)

Currently still in development, the staff and students will have access to a Remote Desktop Services (RDS) system to be used on and off-site. The system will allow them the same access as any workstation in school. Sixth form are also allowed monitored and filtered internet access for personal laptops and devices.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social

networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

- Staff and volunteers 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection
See the school Data Protection Policy.

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 e.g. 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 and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, chat etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to students, parents / careers 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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. The school policy restricts usage as follows:

		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 (e.g. 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 e.g. YouTube		x				

Responding to incidents of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Incidents:

- Concerns about a member of staff should be reported directly to the Headteacher
- Concerns about the conduct of a student should be reported to the appropriate member of staff via the Bromcom system (tutor / curriculum leader / college leader)
- Concerns about the safety or welfare of a student should be recorded on a green form
- Concerns about the Headteacher should be reported to the Chair of Governors (see the school Whistle Blowing policy)

School Actions & Sanctions

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:

	Actions / Sanctions								
Incidents involving a student:	Refer to class teacher / tutor	Refer to Head of Department / Head	Refer to Headteacher	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 e.g. 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		
Unauthorised use of non-educational sites during lessons	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	
Allowing others to access school / academy network by sharing username and passwords	x					x			
Attempting to access or accessing the school / academy network, using another student's / pupil's account	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
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
Continued infringements of the above, following previous warnings or sanctions	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
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	
Deliberately accessing or trying to access offensive or pornographic material	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

Incidents involving a member of staff:	Refer to line manager	Refer to Headteacher, follow safeguarding	HR	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x
Inappropriate personal use of the internet / social media / personal email	x			
Unauthorised downloading or uploading of files	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			
Careless use of personal data e.g. holding or transferring data in an insecure manner			x	
Deliberate actions to breach data protection or network security rules		x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x		
Actions which could compromise the staff member's professional standing		x		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		x		
Using proxy sites or other means to subvert the school's / academy's filtering system	x			
Accidentally accessing offensive or pornographic material and failing to report the incident	x			
Deliberately accessing or trying to access offensive or pornographic material		x		x
Breaching copyright or licensing regulations	x			
Continued infringements of the above, following previous warnings or sanctions		x		