

Policy Title: Online Safety Policy

Statutory

Drafted by:	S Dutton-Johnson (Trust Safeguarding Compliance Officer)
Date of approval by Trust Board:	21.11.16
Review Date:	November 2018
Responsible for Weekly Monitoring:	N Broomhall – Safeguarding Governor - SNF J Conlon – Safeguarding Governor - STBA

UNITED ENDEAVOUR TRUST

EQUALITY CHECKED

This policy/procedure seeks to:

- ① Eliminate unlawful discrimination, harassment and victimisation
- ① Advance equality of opportunity between different groups
- ① Foster good relationships between groups
- ① Meet requirements under the Equality Duty
- ① Set Equality objectives which are specific and measurable



Contents

Development / Monitoring / Review of this Policy	4
Schedule for Development / Monitoring / Review	4
Scope of the Policy	4
Roles and Responsibilities.....	5
Governors / Board of Directors:.....	5
Principal and Senior Leaders:	5
Designated Safeguarding Lead (DSL):.....	6
Network Manager / Technical staff:.....	7
Teaching and Support Staff	7
Students:.....	8
Parents / Carers.....	8
Community Users.....	9
Policy Statements.....	9
Education – Students	9
Education – Parents / Carers.....	10
Education – The Wider Community	10
Education & Training – Staff / Volunteers.....	11
Training – Governors / Directors	11
Technical – infrastructure / equipment, filtering and monitoring	11
Mobile Technologies (including BYOD/BYOT)	13
Use of digital and video images.....	14
Data Protection	15
Communications	17
Social Media - Protecting Professional Identity	18
Unsuitable / inappropriate activities	20
Responding to incidents of misuse	21
Illegal Incidents.....	22

Other Incidents	23
School / Academy Actions & Sanctions	24
Appendix	28

SWGfL / UK Safer Internet Centre

The South West Grid for Learning Trust is an educational trust that has an international reputation in supporting schools with online safety. SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. The Safer Internet Centre is, for example, responsible for the organisation of Safer Internet Day each February. More information about UKSIC services and resources can be found on the website: www.saferinternet.org.uk. SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety) and has spoken at conferences across Europe, America and Africa.

This policy has been adapted from the template provided by SWGfL

Monitoring of the Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
 - students
 - parents / carers
 - staff

Scope of the Policy

This policy applies to all members of the academy community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the

deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy 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 Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy:

Governors / Board of Directors:

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

- regular meetings with the Safeguarding Compliance Officer and Designated Safeguarding Lead (DSL)
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / Committee / meeting

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead.
- The Principal, other members of the Senior Leadership Team and the Safeguarding Compliance Officer should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant disciplinary procedures).

- The Principal / Safeguarding Compliance Officer are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / Safeguarding Compliance Officer will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online 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 / Safeguarding Compliance Officer will receive regular monitoring reports from the DSL.

Designated Safeguarding Lead:

Should be trained in Online 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

The designated lead:

- takes day to day responsibility for online safety issues and has a role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online 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 online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / Technical Staff are responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements
- 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal Safeguarding Compliance Officer for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Principal / Safeguarding Compliance Officer / DSL for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy 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 academy digital technology 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 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 online safety practice when using digital technologies out of school and realise that the academy's Online 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. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good online 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 academy (where this is allowed)

Community Users

Community Users who access academy systems / website as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to academy systems.

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 online safety is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online 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 on-line 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
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- 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 academy.
- 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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 online 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 academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk)
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- The academy website will provide online safety information for the wider community

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Safeguarding Compliance Officer / DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- Safeguarding Compliance Officer / DSL will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in academy training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy 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 online safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- All users will be provided with a username and secure password by technical staff 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 “administrator” passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (eg academy safe)
- The Head of IT Services 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. Illegal content (child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list. 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
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided enhanced / differentiated user-level filtering
- Academy 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 Head of IT Services.
- 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 academy systems and data. These are tested regularly. The academy 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” (eg 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) 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 (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- The school Acceptable Use Agreements for staff, students and parents/carers will give consideration to the use of mobile technologies
- The academy allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No ²	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes		Yes	
No network access				Yes	Yes	Yes

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.

- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect

¹ Authorised device – purchased by the student/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

² The use of mobile / personal devices in school

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 academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy 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 academy 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.
- Student's work can only be published with the permission of the student and parents or carers.

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.

The academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

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" / have "locked" the screen at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to the academy	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 academy , or on academy network				x				x
Use of academy 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 / academy considers the following as good practice:

- The official academy 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 academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).

- Users must immediately report, to the Head of IT Services – in accordance with the academy 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, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students will be provided with individual academy email addresses for educational use.
- Students should be taught about online 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 academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 academy or Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the academy through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Academy staff should ensure that:

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

When official academy social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school / academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the academy are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The academy permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the academy / Trust
- The school should effectively respond to social media comments made by others according to a defined policy or process

The academy's use of social media for professional purposes will be checked regularly by the Head of IT and Safeguarding Compliance Officer to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in a academy context and that users, as defined below, should not engage in these activities in / or outside the school / academy when using academy equipment or systems. The academy 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					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	
	Promotion of extremism or terrorism				X	

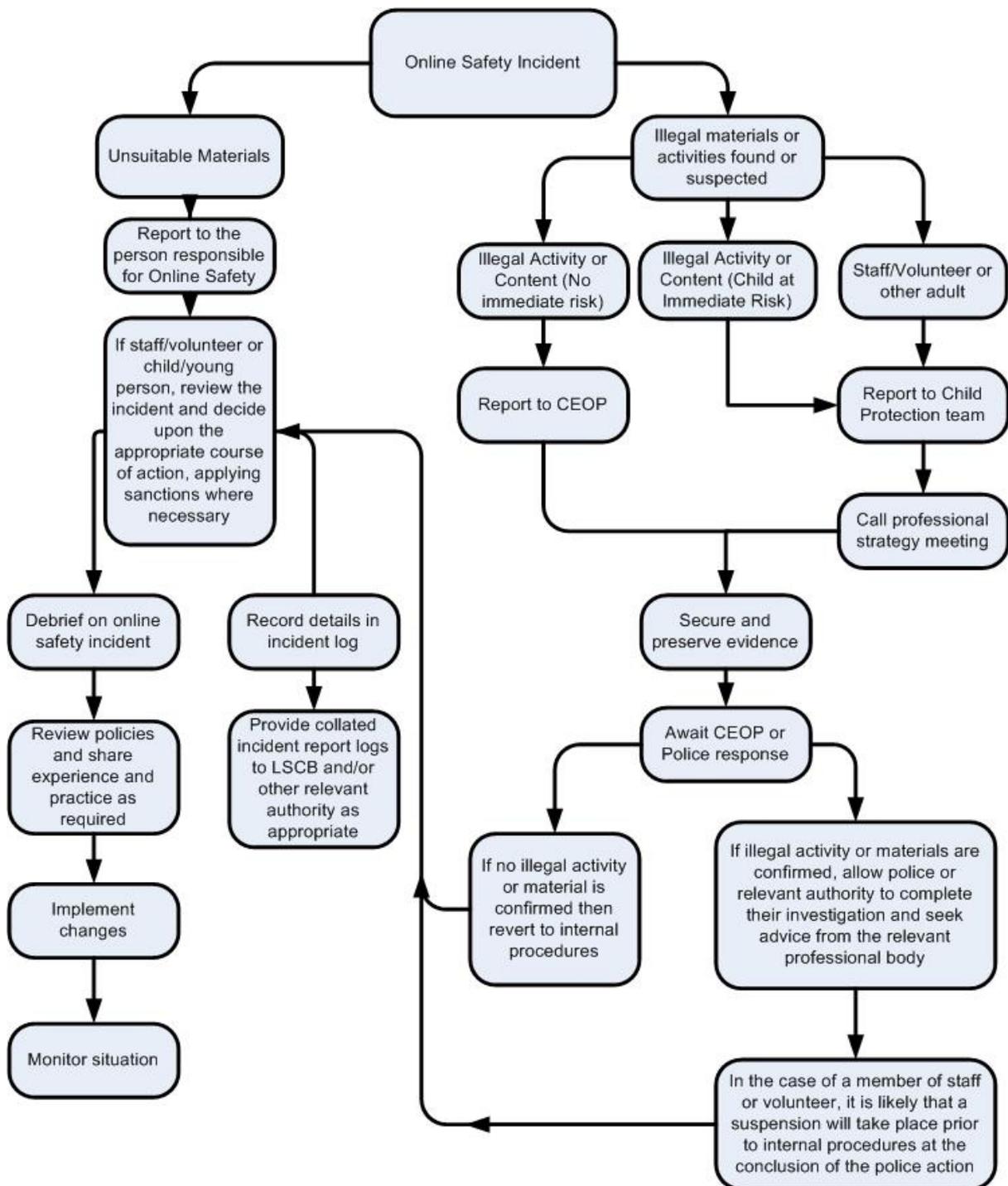
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards 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)					
On-line gaming (non-educational)					
On-line gambling					
On-line shopping / commerce					
File sharing					
Use of social media					
Use of messaging apps					
Use of video broadcasting e.g. Youtube					

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).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority / Academy Trust.
 - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School / Academy Actions & Sanctions

It is more likely that the academy 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:

Students Incidents	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Head of Department / House	Refer to 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
Unauthorised use of non-educational sites during lessons	x	x			x	x		x	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	x				x		x	
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x			X	x	x	x	
Unauthorised downloading or uploading of files		x			x		x	x	x

Allowing others to access academy network by sharing username and passwords		x	x		x	x			x
Attempting to access or accessing the academy network, using another student's account		x	x		x	x		x	
Attempting to access or accessing the 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	x
Continued infringements of the above, following previous warnings or sanctions		x	x		x	x			x
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		x	x		x	x	x		x
Using proxy sites or other means to subvert the 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	
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	x	x

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to 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
Inappropriate personal use of the internet / social media / personal email		X			X	X		
Unauthorised downloading or uploading of files	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
Careless use of personal data e.g. 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
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		X	X	X			X	X
Actions which could compromise the staff member's professional standing		X	X				X	X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		X						X
Using proxy sites or other means to subvert the academy's filtering system		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
Breaching copyright or licensing regulations		x				x		
Continued infringements of the above, following previous warnings or sanctions		x	x	x			x	x

Appendices

Legislation.....	29
Links to other organisations or documents	34
Glossary of Terms	37

Relevant legislation:

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless

anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - Ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation.

Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel

to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connections staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

UK Safer Internet Centre

Safer Internet Centre – <http://saferinternet.org.uk/>

South West Grid for Learning - <http://swgfl.org.uk/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - <http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work>

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012 \(England\)](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO Subject Access Code of Practice](#)

[ICO – Guidance on Data Security Breach Management](#)

SWGfL - [Guidance for Schools on Cloud Hosted Services](#)

LGfL - [Data Handling Compliance Check List](#)

Somerset - [Flowchart on Storage of Personal Data](#)

NEN - [Guidance Note - Protecting School Data](#)

Professional Standards / Staff Training

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](#)

[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure / Technical Support

Somerset - [Questions for Technical Support](#)

NEN - [Guidance Note - esecurity](#)

Working with parents and carers

[SWGfL Digital Literacy & Citizenship curriculum](#)

[Online Safety BOOST Presentations - parent's presentation](#)

[Connectsafely Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

[Ofcom – Children & Parents – media use and attitudes report - 2015](#)

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes).
CPD	Continuous Professional Development
FOSI	Family Online Safety Institut
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)

SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Fo

EQUALITY IMPACT ASSESSMENT POLICY CHECKLIST

Equality Impact Assessment of SNT Policy																																																													
Title of Policy	Online Safety Policy																																																												
PART 1	Positive Impact – reducing inequalities																																																												
Statutory duty/equality legislation: Equality Impact Assessment undertaken or is satisfied. D = Disability, GA = Gender reassignment, P = Pregnancy & Maternity, R = Race, R/B = Religion or Belief, S = Sex, SO = Sexual Orientation, A = Age, M/CP = Marriage and Civil Partnerships	<p>How is the policy likely to have a <u>significant positive impact</u> on equality by reducing inequalities that already exist?</p> <p>All students and staff will be provided with awareness raising in this area and will be given opportunities to access support if required.</p> <p>Could the policy have a <u>significant negative impact</u> on equality in relation to each of the following groups or characteristics?</p> <p>No.</p>																																																												
Characteristics Indicate areas of likely impact	<table border="1"> <thead> <tr> <th>Promote equal opportunities</th> <th>Get rid of discrimination</th> <th>Get rid of harassment</th> <th>Promote good community relations</th> <th>Promote positive attitudes</th> <th>Promote/ protect human rights</th> </tr> </thead> <tbody> <tr> <td>✓</td> <td>✓</td> <td>✓</td> <td></td> <td></td> <td>✓</td> </tr> </tbody> </table>	Promote equal opportunities	Get rid of discrimination	Get rid of harassment	Promote good community relations	Promote positive attitudes	Promote/ protect human rights	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓			✓	✓	✓	✓			✓
Promote equal opportunities	Get rid of discrimination	Get rid of harassment	Promote good community relations	Promote positive attitudes	Promote/ protect human rights																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
✓	✓	✓			✓																																																								
Equality Impact Assessment of SNT Policy	Records																																																												
Name of person responsible for policy	S Dutton Johnson																																																												
Date of EIA of Policy	6.11.17																																																												

A = Age, M/CP = Marriage and Civil Partnerships –applies in respect of employment framework policies

Equality Impact Assessment of SNT Policy	Evidence
PART 2	
<p>Statutory duty/equality legislation: Equality Impact Assessment undertaken or is satisfied.</p> <p><i>D = Disability, GA = Gender reassignment, P = Pregnancy & Maternity, R = Race, R/B = Religion or Belief, S = Sex, SO = Sexual Orientation,</i></p> <p><i>A = Age, M/CP = Marriage and Civil Partnerships</i></p>	<p>What is the evidence for your answers above? (list any quantitative and qualitative)</p> <p>Full records are kept of any incident dealt with.</p> <p>Report to CEO/ Governors/Directors via termly report.</p>

Equality Impact Assessment of SNT Policy	Conclusion
<p style="text-align: center;">PART 3</p> <p>Summary of findings</p>	Current evaluation indicates that concerns are addressed quickly and effectively, but that there are issues that affect specific groups.

Equality Impact Assessment of SNT Policy	Next steps		
PART 4			
Category	Actions	Target Date	Person responsible
Next Steps – Action Plan			
Practical changes required to reduce adverse impact	Continue to raise awareness of Online safety. Record, address and evaluate responses.	On going	S Dutton Johnson
Monitoring and evaluation and Review (publish revised policy)	Outcomes reported to SLT / Governors / Directors via report	November 2018	S Dutton Johnson