E-SAFETY POLICY

Policy Reference No	IT002
Review Frequency	Annual
Reviewed	Spring 2020
Next Review Date	Summer 2021
Ratified by SET	

TOGETHER WE EMPOWER EXCELLENCE

Contents:

Introduction

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to/loss of/sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

1. Policy Document

This policy applies to all members of the Trust community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of the Trust's ICT systems, both in and out of our academies.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils 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 out of the Academy, but is still linked to membership of the Academy. The Trust will deal with such incidents within this policy and associated behaviour and inappropriate e-safety behaviour that take place out of school. Parents/carers may be informed of concerns via telephone or letter.

2. Roles and Responsibilities

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

Trust Executive Team

Trust Executive Team are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Head of Academy and Senior Leaders

- Chief Executive Officer and Head of Academy are responsible for ensuring the safety (including e-safety) of members of their Academy communities;
- Chief Executive Officer, Head of Academy and senior leaders are responsible for ensuring that relevant staff receive suitable training and development to enable them to carry out their e- safety roles and to train other colleagues, as relevant;
- Chief Executive Officer, Head of Academy and senior leaders will ensure that there is a system in place to allow for the monitoring and support of those in the academies who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support those colleagues who take on important monitoring roles;
- Each Academy's senior leadership team (SLT) will receive information regarding any e-safety incidents which will be logged and reviewed during SLT meetings;
- Chief Executive Officer, Head of Academy and members of each Academy 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.

Member of SLT with responsibility for e-safety

- Take day to day responsibility for e-safety issues and oversee the sanctions for breaches of rules relating to e-safety;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Provide training and advice to staff;
- Liaise with the Local Authority Designated Officer (LADO) or Police as appropriate;
- Liaise with the Trust's ICT technical staff;
- Receive reports of e-safety incidents as part of behaviour monitoring;
- Provide information to the Trust's Executive Team/Board as appropriate.

ICT Manager/ICT Technical Staff

- Ensure that the Academy and Trust ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the Trust's ICT systems are secure, in line with the Trust's guidance and policies.

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of current Trust e-safety policy and practices;
- They have read and understood the appropriate ICT agreements;
- They report any suspected misuse or problem to a member of SLT;
- Digital communications with pupils are only on a professional level and carried out using official Trust systems;
- It is understood that social media can play an important part in communication between the Trust and pupils, parents/carers; however, there is also a need to ensure it is used in an appropriate and safe way. Before any member of staff sets up a resource such as a pupil blog space, they must seek permission from the Head of Academy and they should ensure that appropriate steps are taken to make such social media 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from other users/contributors;
- E-safety issues are embedded in all aspects of the curriculum and other academy activities;
- Pupils understand and follow the Trust's e-safety and Acceptable Use Policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extra-curricular and extended Academy activities;
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current best practice with regard to these devices;
- In lessons where internet use is pre-planned, pupils should be guided to sites that are checked as suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for serious child protection 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

Pupils

- Are responsible for using the Trust's ICT systems in accordance with Trust policy, which they will be expected to sign for before being given access to the Trust systems;
- 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 Trust policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand the Trust's 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 Trust E-Safety Policy covers their actions out of the academies, if related to their membership of the Trust.

Parents/Carers

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

Parents/carers and volunteers will be responsible for:

- Endorsing the Trust policy;
- Accessing the Academy website in accordance with the relevant Acceptable Use Policy.

3. Education and Training

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

- A planned e-safety programme will be provided as part of the ICT programme;
- Key e-safety messages will be reinforced as part of a planned programme of

assemblies and within the PSHE curriculum;
- Pupils will be taught whenever an opportunity occurs to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information;
- Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the academies;
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

Education and Training – Staff

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

- E-safety training for all staff is undertaken on an annual basis. Further e-safety training will be included as part of staff' child safeguarding training;
- All new staff will receive e-safety training as part of their induction programme, ensuring they understand the E-safety Policy and Acceptable Use Policy.

Training – Trustees

The Trust's annual Child Safeguarding and Prevent training covers the relevant elements of e-safety training. Trustees are required to undertake the Trust's Safeguarding Children and Prevent Training on an annual basis.

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site, VLE
- Parents evenings
- Reference to websites such as the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents), ThinkuKnow, Torbay Virtually Safe, Devon.gov.uk
- Termly E-Safety Weeks incorporating termnly special parents assemblies

4. Infrastructure, equipment, filtering and monitoring

The Trust will be responsible for ensuring that the academies infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- All users will have clearly defined access rights to Trust's ICT systems;
- All staff users will be provided with a username and password by ICT support who will keep an up to date record of users and their usernames. Users will be required to change their password regularly;
- All pupil users (above KS1) will be provided with a username and password by (systems manager) who will keep an up to date record of users and their usernames. Users will learn how to change their password regularly as part of their curriculum learning.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- In the event of the IT Manager (or other member of the IT Support Team) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head of Academy or Chief Executive Officer;
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager;
- ICT technical staff regularly monitor and record the activity of users on the Trust's ICT systems and users are made aware of this in the Acceptable Use Policy;
- Remote management tools are used by staff to control workstations and view users' activity;
- An appropriate system is in place for users to report any actual / potential e- safety incident to SLT;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the Trust's systems and data;
- The "master / administrator" passwords for the school ICT system, used by the Systems Manager (or other person) must also be available to the Chief Executive Officer or other nominated senior leader and kept in a secure place (e.g. school safe)
- Guest users may be granted a temporary log in or guest account if agreed by the IT Manager;
- Personal use of the Trust's ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes;
- Neither staff nor pupils should install programmes or other software on workstations, portable devices or servers, without the prior express, written permission of the academy's IT Manager;

- Each Academy's ICT infrastructure and individual workstations are protected by up to date virus software;
- Personal data (as defined by the Data Protection Act) cannot be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured by password or other means – please refer to the Trust's Data Handling Policy for further information;
- Where staff have email accounts and other Trust data on their phone or other mobile device they must ensure that the device is locked with a password.

5. Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, e.g. using search engines, 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, pupils 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 Network Manager (and other relevant 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.
- Pupils 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;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

6. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The Trust will inform and educate users about these risks and implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils 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.

- Staff are allowed to take digital / video images to support educational aims, but must follow Trust policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Trust equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Trust into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the Trust's Photograph and Video policy
- Pupils' 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 pupils are published on the academy website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

7. GDPR (General Data Protection Regulation)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

The seven data protection principles as laid down in the GDPR are followed at all times:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- Personal data shall be collected for specific, explicit, and legitimate purpose, and shall not be further processed in a manner incompatible with those purposes;
- Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
- The Trust is responsible for complying with GDPR and must be able to demonstrate compliance.

Staff must ensure that they:

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

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

- the data must be encrypted and password protected;
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected, if this is the case then each individual file will need to be password protected);
- the data must be securely deleted from the device, once it is no longer required.

8. Communications

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

	Staff & other adults			Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				

Use of mobile phones in social time	X							
Taking photos on mobile phones or other camera devices				X				
Use of Trust devices eg PDAs, PSPs		X						
Use of personal email addresses in school, or on school network				X				
Use of school email for personal emails				X				
Use of chat rooms / facilities				X				
Use of instant messaging				X				
Use of social networking sites				X				
Use of blogs				X				

The Trust considers the following as good practice:

- The official Trust email service may be regarded as safe and secure and is monitored. Staff and Pupils should therefore use only the academy email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications are monitored
- Users must immediately report, to the nominated person – in accordance with the Trust policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE 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 public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses may be used at KS1, while pupils at KS2 and above may be provided with individual school email addresses for educational use. This will be on request and limited to a brief time so that out of school hours, contact can not be made between others using a child's account to contact another child or parent..

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- The use of educational streaming video clips such as Youtube is acceptable for up to 10 minutes at a time. Videos should be checked prior to screening by an adult. The video should be documented prior to the lesson and not allowed to auto run into the next video. Videos should be shown in full screen so to minimize any comments surrounding the video. An adult should be with children when they are watching clips.

9. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from the Trust and all other ICT systems. Other activities e.g. Cyber-bullying, use of electronic communications to radicalise children or others, is 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 school context, either because of the age of the users or the nature of those activities.
School policy restricts certain internet usage as follows:

User Actions	Acceptability	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				X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation				X
	adult material that potentially breaches the Obscene Publications Act in the UK				X
	criminally racist material in UK				X
	pornography				X
	promotion of any kind of discrimination				X

	promotion of racial or religious hatred				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	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				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	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and 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 networking sites		X			
Use of video broadcasting eg Youtube.		X			
The use of on demand film sites such as Netflix, Amazon, Now TV and DisneyLife in schools when using a personal account.					X
The downloading & storage of video clips e.g youtube clips					X

10. Responding to incidents of misuse

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

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

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

Remove pupils, staff and others from exposure to the material and immediately notify the Chief Executive Officer (or nominated individual in her absence) who should then contact the police. Further action should be agreed with the police.

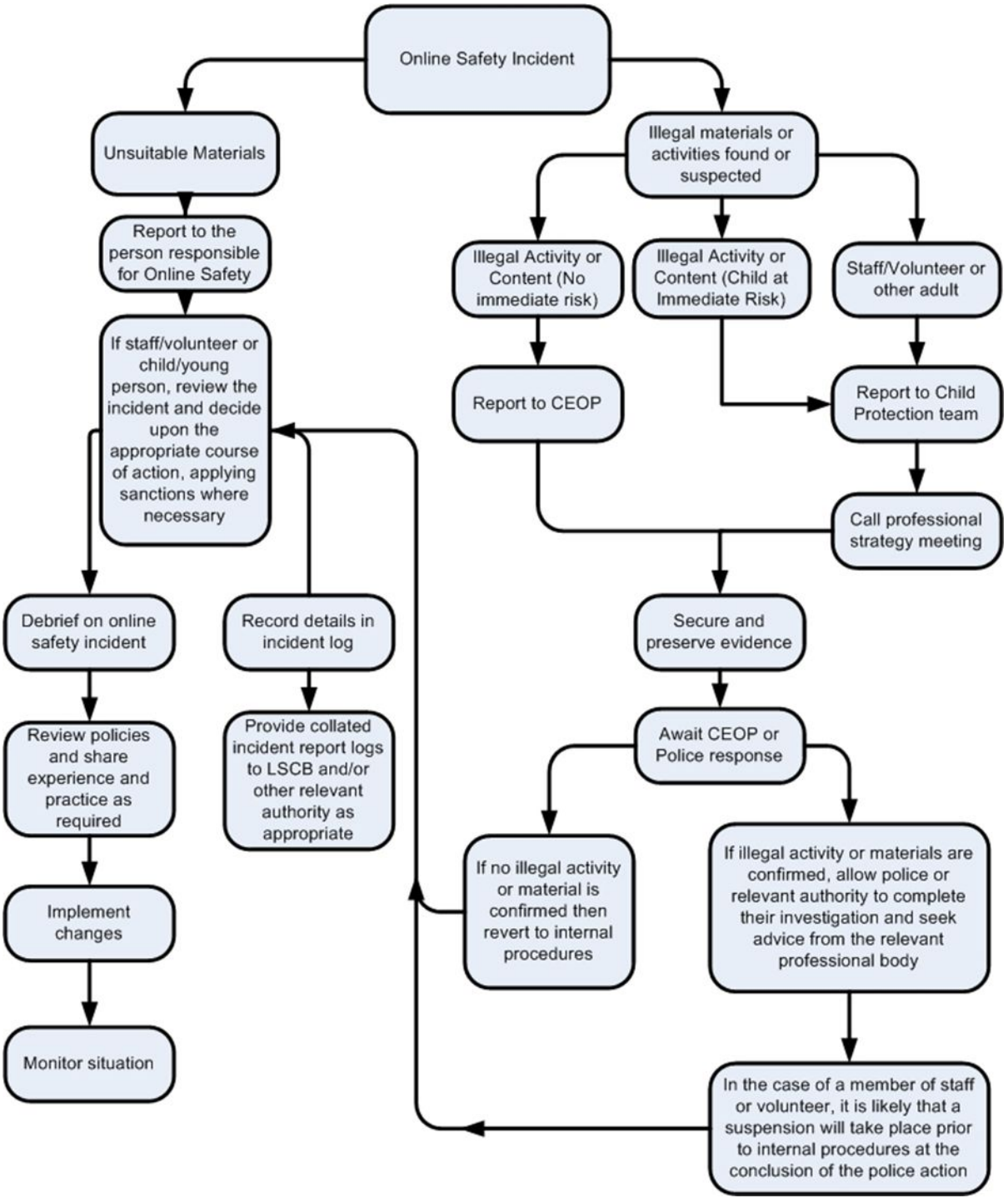
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

In such event the SWGfL “Procedure for Reviewing Internet Sites for Suspected Harassment and Distress” should be followed. This can be found on the SWGfL Safe website within the “Safety and Security booklet”. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer. (see flow chart below for this)

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:

Flowchart for responding to online safety incidents



Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Academy	Refer to Chief Executive Officer	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X	
Unauthorised use of non-educational sites during lessons	X				X			X	
Unauthorised use of mobile phone / digital camera / other handheld device	X				X			X	
Unauthorised use of social networking / instant messaging / personal email	X	X			X		X	X	
Unauthorised downloading or uploading of files	X				X			X	
Allowing others to access school network by sharing username and passwords	X				X		X	X	
Attempting to access or accessing the school network, using another pupil's account		X			X		X	X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X		X	X	
Corrupting or destroying the data of other users		X			X		X	X	
Sending an email, text or instant 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 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 filtering system		X			X		X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X		X	X	

Staff Actions / Sanctions

Incidents:	Refer to Head of Academy	Refer to Chief Executive Officer	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X				X	X		
Unauthorised downloading or uploading of files	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 eg holding or transferring data in an insecure manner	X				X	X		
Deliberate actions to breach data	X	X			X			X

protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X			X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X			X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with Pupils	X	X			X	X	X	X
Actions which could compromise the staff member's professional standing	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		
Using proxy sites or other means to subvert the school's filtering system	X				X	X		
Accidentally accessing	X	X			X	X		

offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material	X	X			X		X	X
Breaching copyright or licensing regulations	X	X			X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X			X		X	X

Appendix 1: E-Safety – A School Charter for Action

Name of School

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

Our school community

Discusses, monitors and reviews our e-safety policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole school curriculum.

Ensures that pupils are aware, through e-safety education, of the potential e-safety risks associated with the use of ICT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's e-safety policy.

Provides opportunities for parents/carers to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The school will report back to parents / carers regarding e-safety concerns. Parents/carers in turn work with the school to uphold the e-safety policy.

Seeks to learn from e-safety good practice elsewhere and utilises the support of the LA and relevant organisations when appropriate.

Appendix 2: Resources and further information

Devon County Council, Online Safety for Education and Families:
https://www.devon.gov.uk/eycs/for-providers/safeguarding/online-safety/

Torbay Safeguarding Children Partnership:
http://torbaysafeguarding.org.uk/cyp/online-safety/

Practical online safety advice for people in Torbay which aims to keep children safer online: http://www.torbayvirtuallysafe.co.uk/

NSPCC: https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/
https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Think U Know: https://www.thinkuknow.co.uk/

SWGFL: https://swgfl.org.uk/

Appendix 3: Changes

Edits to this document

Date	Details	Initials of editor	Reason for the edit.
April 17	Senior Risk Information Officer (SIRO) changed to Director of Operations from the Business Manager	TET	
	The management of the password security policy will be the responsibility of the IT Manager. Changed from Business Manager	TET	
December 2019	**Replace:** *"Chief Executive Officer (or other nominated senior leader)."* with *"Head teacher of the school"*	AG	To localise responsibility
December 2019	**Replace:** *"SWGfL"* with *"IT Services & directly to the IT Team. The school staff can also contact Vaioni directly in the case…"*	AG	To refer to the Vaioni connections
December 2019	**Delete:** *"An agreed policy is in place regarding the downloading of executable files by users"*	AG	Replicated
December 2019	**Replace:** *"school workstations"* with *"computers"*	AG	User friendly
December 2019	**Add:** *". This will be on request and limited to a brief time so that out of school hours, contact can not b…"*	AG	Update for wifi.
December 2019	**AUPs removed -** To be linked documents to the newly created AUPs	AG	To keep documents synchronized
December 2019	School Filtering policy area rewritten to reflect the Vaioni Connections.	AG	Update on new process
December 2019	**Replace:** *"South West Grid for Learning (SWGfL) schools"* with *"Vaioni supplied Fortinet filtering service"*	AG	Update to new process
December 2019	**Replace:** *"five"* **with** *"15"*	AG	correction
December 2019	**Add:** *"Teaching devices are set to lock after 30 minutes inactivity to allow classes to run correctly"*	AG	New item as teacher devices are also a portal to confidential DATA
December 2019	**Replace:** *"SIRO"* **with** *"DPO"*	AG	Update to structure
December 2019	**Replace:** *"School"* **with** *"Trust"*	AG	Required Update

December 2019	**Add:** *"*Please identify your role / position STAFF - TRUSTEE - VOLUNTEER - VISITOR*"*	AG	On AUP
JANUARY 2020	REMOVED AUP FOR STUDENTS	AG	DUPLICATED ELSEWHERE
JANUARY 2020	REMOVED AUP FOR PARENTS & CARERS	AG	DUPLICATED ELSEWHERE
JANUARY 2020	REMOVED AUP FOR STAFF, TRUSTEES, VOLUNTEERS & VISITORS.	AG	DUPLICATED ELSEWHERE
JANUARY 2020	Appendices MENU UPDATED	AG	TO REFLECT CHANGES
February 2020	Reworked by DSL to be more E-Safety than Technical	LQ	Aiming to be more E-Safety than Technical
February 2020	School Filtering Policy	AG	REMOVED AND PLACED INTO COMPUTER SECURITY POLICY
February 2020	School Password Security Policy	AG	REMOVED AND PLACED INTO COMPUTER SECURITY POLICY
February 2020	School Personal Data Handling Policy	AG	REMOVED AS GDPR COVERS THIS IN A SEPARATE POLICY