Online Safety Policy

Camborne Science and International Academy

Approved by:	Governors' Policy Committee	**Date:** 6th December 2019
Last reviewed on:	11th December 2018	
Next review due by:	December 2020	

All CSIA policies are reviewed by the Governors' Policy Committee (which meets termly), according to a fixed schedule. On extremely rare occasions, there may be circumstances where an event (for example, a change in legislation/national guidance), necessitates a policy being amended immediately, outside of this schedule. Where this is necessary, the Principal will seek permission from the Chair of the Governors' Policy Committee, to amend the policy immediately. The Principal will then confirm details of any amendments with all members of the committee by email and the policy will be reviewed at the next scheduled meeting of the committee.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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 to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student 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.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg Behaviour for Learning, Anti-bullying and Child Protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' 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.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

This online safety policy has been developed by the Online Safety Working Party, made up of:

- Mark Fenlon – Vice Principal and Designated Safeguarding Lead
- Tim Stuka – Network Manager
- Susan Gellatly – PSHE Coordinator
- Tom Smith – Director of Faculty for Computing, Economics and Business
- Clare Harvey – Governor

Mark Fenlon's role in the Online Safety Working Party is to:

- Lead the Online Safety Working Party in his role as Senior Designated Safeguarding Lead and Online Safety Coordinator.
- Communicate online safety issues or trends with the other members of the Online Safety Working Party.
- Act as the online safety link to the SLT through his role as Vice Principal.
- Collate, investigate and where necessary to act upon reported incidents in his capacity as Designated Safeguarding Lead, or where appropriate to distribute and oversee these actions where they are able to be performed by other members of staff.
- Take accumulated records of incidents to Clare Harvey, Online Safety and Chair of Governors on an annual basis to provide an overview of trends and a clear understanding of online safety in the school.
- Review the effectiveness of the schools online safety policy annually.

Tim Stuka's role in the Online Safety Working Party is to:

- Communicate online safety issues or trends with the other members of the Online Safety Working Party.
- Oversee the filtering and security of our school network, to determine and manage network bans or other sanctions where they need to be applied, in his capacity as Network Manager.

Susan Gellatly's role in the Online Safety Working Party is to:

- Support with the delivery of online safety training for students through the Citizenship program and PSHE days.
- Evaluate the impact of the delivery of online safety training for students.

Tom Smith's role in the Online Safety Working Party is to:

- Communicate online safety issues or trends with the other members of the Online Safety Working Party.
- Attend online safety training events and update other members of the Online Safety Working Party regarding new threats.
- Update the online safety policy in reaction to changes in technologies, changes in other school policies (i.e. behavioural policies) or trends in use.
- Manage the delivery of online safety training for students, staff and parents/carers.
- Evaluate the impact of the delivery of online safety training for students, staff and parents/carers.

Consultation with our school community in the development of this document has taken place through the following:

- Students consulted through the Student Council
- Parents through publication on the school website
- Teachers through policy development consultation
- Governors through policy development consultation

Development/Monitoring/Review Schedule

This online safety policy was approved by the Governing Body :	December 2019
The implementation of this online safety policy will be monitored by:	• Mark Fenlon – Vice Principal and Designated Safeguarding Lead • Tim Stuka – Network Manager • Tom Smith – Director of Faculty for Computing, Economics and Business • Susan Gellatly – Director of Citizenship and PSHE
Monitoring will take place at regular intervals:	Continuously, in response to identified risks and at the start of each academic year.
The Policy Review Committee will review the policy annually and ensure the Governing Body are kept updated on online safety actions implemented by the school.	At the start of each academic year.
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	December 2020
Should serious online safety incidents take place, the following external persons are to be informed:	• Mark Fenlon – Vice Principal and Designated Safeguarding Lead • CEOP • Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Internal real time monitoring of computer use
- Surveys/questionnaires of students/parents/carers (i.e. CEOP Think U know before and after training survey)

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents as stated within this policy, and will where necessary, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Governors Roles and Responsibilities:
Governors 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 who will receive annually, information about online safety incidents and monitoring reports.

The Governing Body has a specific governor (Clare Harvey) who takes responsibility for Safeguarding (including online safety). The role of this governor includes:

- Attending meetings with the Online Safety Working Party.
- Monitoring of online safety incident logs (provided by the Online Safety Working Party)
- Monitoring of filtering/change control logs (provided by the Online Safety Working Party).
- Reviewing any required changes to the online safety policy.
- Reporting back to the Governing Body.

Principal and Senior Leaders Roles and Responsibilities:

- The Principal is responsible 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 Online Safety Working Party.
- The Principal/Senior Leaders are responsible for ensuring that the Online Safety Working Party and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal 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 will receive regular monitoring reports from the Online Safety Working Party.
- The Principal and another member of the Senior Leadership Team 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 SWGfL flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

Online Safety Coordinator Roles and Responsibilities:

- Leads the Online Safety Working Party.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy.
- 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 opportunities for training and advice for staff.
- Liaises with the Local Authority.
- Liaises with school ICT technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with the online safety governor and Online Safety Working Party to discuss current issues, review incident logs and filtering/change control logs.
- Reports annually to Senior Leadership Team and Governors.
- Decides how specific incidents will be dealt with.
- Applies investigation/action/sanctions.
- Is trained in online safety issues and is aware of the potential for serious child protection issues to arise from sharing of personal data, accessing illegal/inappropriate materials, inappropriate on-line contact with adults/strangers, potential or actual incidents of grooming, cyber-bullying.

Network Manager/Technical staff Roles and Responsibilities:

- Ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Ensures that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority online safety policy and guidance.
- Ensures that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Ensures that SWGfL is informed of issues relating to the filtering applied by the Grid
- Ensures that the school's filtering policy is applied and that it is updated on a regular basis.
- Ensures that he keeps up to date with online safety technical information in order to effectively carry out his online safety role, and to inform and update his team as required.
- Ensures that the use of the network/Virtual Learning Environment/remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Coordinator or another member of the Senior Leadership team for investigation/action/sanction.
- Ensures that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff Roles and Responsibilities:

- Ensuring that they have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- Ensure they have read, understood and signed the school Staff Acceptable Use Policy, including that staff do not allow students to access the school network through their login/password.
- Ensure they report any suspected misuse or problem to a member of the Online Safety Working Party for investigation/action/sanction.
- Ensure digital communications with students (email/Virtual Learning Environment/voice) should be on an academic level and only carried out using official school systems.
- Ensure online safety issues are embedded in all aspects of the curriculum and other school activities.
- Ensure students/pupils understand and follow the school online safety and students acceptable use policy.
- Ensure they monitor ICT activity in lessons, extra curricular and extended school activities.
- Ensure they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

Online Safety Working Party Roles and Responsibilities:
Members of the Online Safety Working Party will work to assist the Online Safety Coordinator through:

- The production/review/monitoring of the school online safety policy and documentation.
- The production/review/monitoring of the school filtering policy.
- Ensuring information regarding new developments are passed on effectively, in order to take a cohesive approach to online safety within the committee.

Students Roles and Responsibilities:

- Responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents & Carers Roles and Responsibilities:
Parents & Carers play a crucial role in ensuring that their children understand the need to use the internet & mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Moodle and information about national / local online safety campaigns/literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy
- Accessing the school website/Moodle/on-line student records in accordance with the school's Acceptable Use Policy.

Community Users Roles and Responsibilities:
Community Users who access school ICT systems/website/Moodle as part of the Extended School provision will be expected to sign a Guest User AUP before being provided with access to school systems.

Policy Distribution

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 school's online safety provision. Students will be supported by the school to recognise and avoid online safety risks.

Education for students about online safety issues will be provided in the following ways:

- A planned online safety programme is provided as part of ICT lessons in year 7 and covers both the use of ICT and new technologies in school and outside school. In year 8 this theme is revisited, and then throughout KS4, teachers make reference to online safety issues where pertinent.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities.
- New threats and initiatives are brought to student's attention through desktop wallpaper messages and CSIA Bulletin.
- Students are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Students are helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students must agree to code-of-conduct displayed on log-on screens before using school computers.
- Advice about online safety issues is displayed on all log-on screens.
- Staff act as role models for safe use of electronic devices.

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 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:

- Newsletters articles
- Distribution of resources (CD ROMs etc.)
- Internet Safety for Parents & Carers events
- The Online Safety section of the CSIA website

Staff

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

- E-safety training will be delivered to staff as INSET. It is expected that some staff will identify online safety as a training need within the performance management process, so additional training is available on request.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.
- The Online Safety Coordinator/Child Protection Officer will receive regular updates through members of the Online Safety Working Party's attendance at SWGfL/LA/other information/training sessions and by reviewing guidance documents released by SWGfL/LA and others.
- This online safety policy and its updates will be presented to and discussed by staff through INSET.
- The Online Safety Working Party will provide advice/guidance/training as required to individuals as required.

Governors

Where appropriate, Governors will receive online safety training sessions, in particular those Governors who are members of a sub committee or group involved in child protection. This is offered in a number of ways:

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

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that:

- The school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- The relevant people named in this policy will be effective in carrying out their online safety responsibilities.
- The school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority online safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded and reviewed accordingly, by the Online Safety Working Party.
- All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every month.
- The administrator passwords for the school ICT system, used by the Network Manager (and technicians) are available to the Principal and are kept in a secure place. Sole administrative access is not in occurrence.
- Users are made responsible for the security of their username and password.
- The school maintains and supports the managed filtering service provided by SWGfL.
- In the event of the Network Manager (or other person) 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 Principal (or other nominated senior leader).
- Any filtering issues should be reported immediately to SWGfL.

- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Working Party.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT.
- An appropriate system is in place for users to report any actual/potential online safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on laptops and other portable devices owned by the school that may be used outside of the school.
- An agreed policy is in place that forbids staff from installing programmes on school workstations or portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations/portable devices
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

Online is a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- 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, eg 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, 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 Network Manager (or technicians) 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.
- Students are 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.
- Where staff require less restricted internet access for VI Form lessons, they have the option to use the BYOD wireless network. This can be done through the booking of iPads or allowing students to use their own devices.

Use of digital and video images - Photographic, Video
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 and students 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 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 eg on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written consent from parents or carers will be obtained before photographs of students are published in any outward facing school publications.
- Student's work is only 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.

As a school we will ensure that:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- We 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.
- We transfer data using encryption and secure password protected devices.

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.
- Where possible 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.

Please refer to the schools Data Protection Policy for further details.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Every school has to weigh up the benefits and risks of using these technologies. The following table shows how CSIA currently considers the use of these technologies:

	Staff & other adults				VI Form Students						
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of mobile phones in lessons				☑			☑			☑	
Use of mobile phones in social time	☑						☑		☑		
Taking photos on mobile phones or other camera devices		☑					☑				☑
Use of hand held devices eg PDAs, PSPs	☑									☑	
Use of personal email addresses in school, or on school network	☑								☑		
Use of school email for personal emails		☑				☑			☑		
Use of CSIA Google Classroom / VLE	☑				☑			☑			
Use of chat rooms / instant messaging / social networking sites				☑			☑				☑
Use of blogs		☑								☑	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems. The use of other email services is permitted, but staff are discouraged and do this at their own risk.
- Staff are to only use e-mail to communicate with students for matters related to academic issues. **All E-mails must :**
    - **contain appropriate/professional dialogue related to purely academic matters and <u>not</u> pastoral matters**
    - **be sent at an appropriate time of the day (8am – 7.30pm UK Time)**
    - **be transparent in nature with no ambiguity**
    - **be limited in dialogue and not an ongoing regular form of communication**
    - **copy in link manager**
- Users are all aware that email communications are monitored and filtered.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature to a member of the Online Safety Working Party, and must not respond to any such email.
- Any digital communication between staff and students or parents/carers (email, blogs, 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.
  Communications on Google Classroom / other VLEs must:
    - **where public (post on the stream), should use professional dialogue and not openly criticize individuals**
    - **where private (feedback on an assignment), be transparent in nature with no ambiguity. Each Google Classroom must add "Google Administrator" and preferably a link manager as a teacher**
    - **be sent at an appropriate time of the day (8am – 7.30pm UK Time)**
- Students are taught about email safety issues, such as the risks attached to the use of personal details. They are also taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Unsuitable/inappropriate activities

Some internet activity (e.g. accessing child abuse images or distributing racist material) is illegal and would therefore result in a ban from all school ICT systems, until proceedings for a criminal investigation had taken place. Other activities (e.g. cyber bulling or accessing pornography) may not be illegal, but are obviously inappropriate in the school context. These activities will lead to a ban from all school ICT systems until the relevant member/s of the Online Safety Working Party have completed an investigation, and the issue is resolved.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					☑
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☑
	adult material that potentially breaches the Obscene Publications Act in the UK					☑
	criminally racist material in UK					☑
	pornography				☑	
	promotion of any kind of discrimination				☑	
	promotion of racial or religious hatred					☑
	threatening behaviour, including promotion of physical violence or mental harm					☑
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☑	
Using school systems to run a private business					☑	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					☑	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					☑	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					☑	

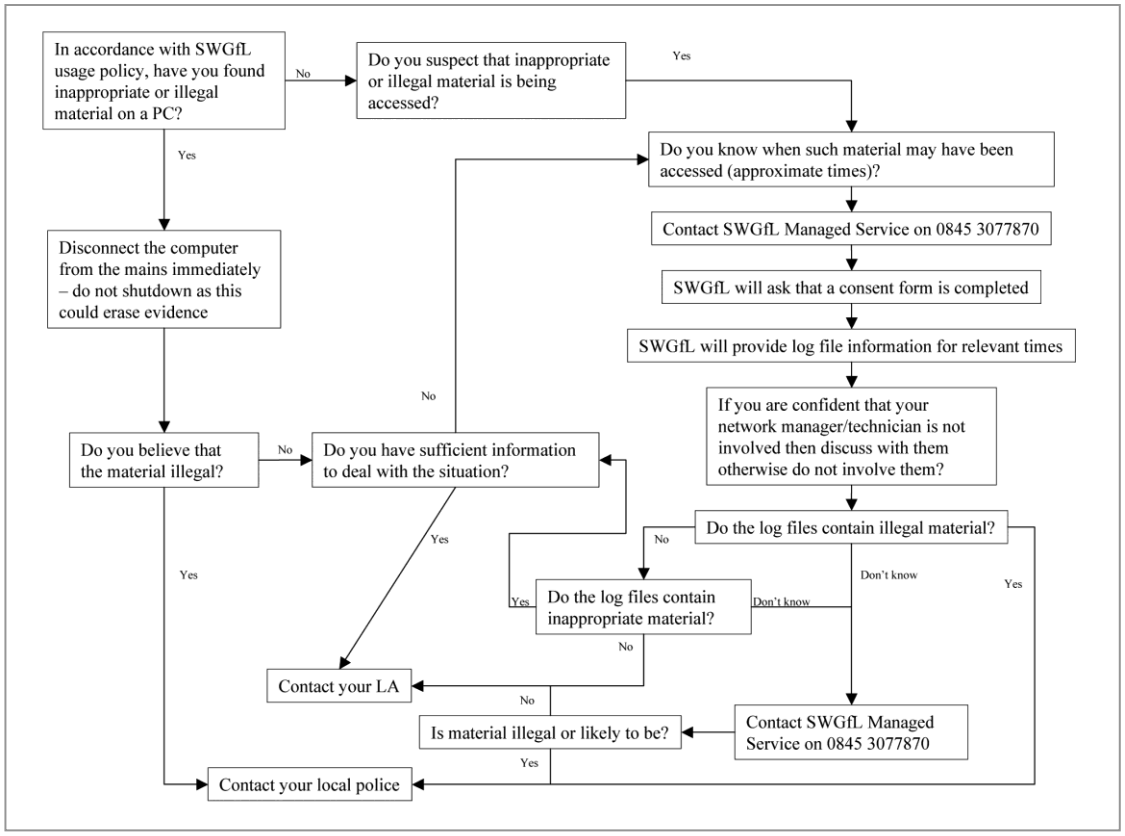
Creating or propagating computer viruses or other harmful files				☑	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☑	
On-line gaming (educational)		☑			
On-line gaming (non educational)				☑	
On-line gambling					☑
On-line shopping / commerce			☑		
File sharing				☑	
Use of social networking sites				☑	
Use of video broadcasting eg Youtube			☑		

Responding to incidents of misuse

It is expected 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:

Illegal activity

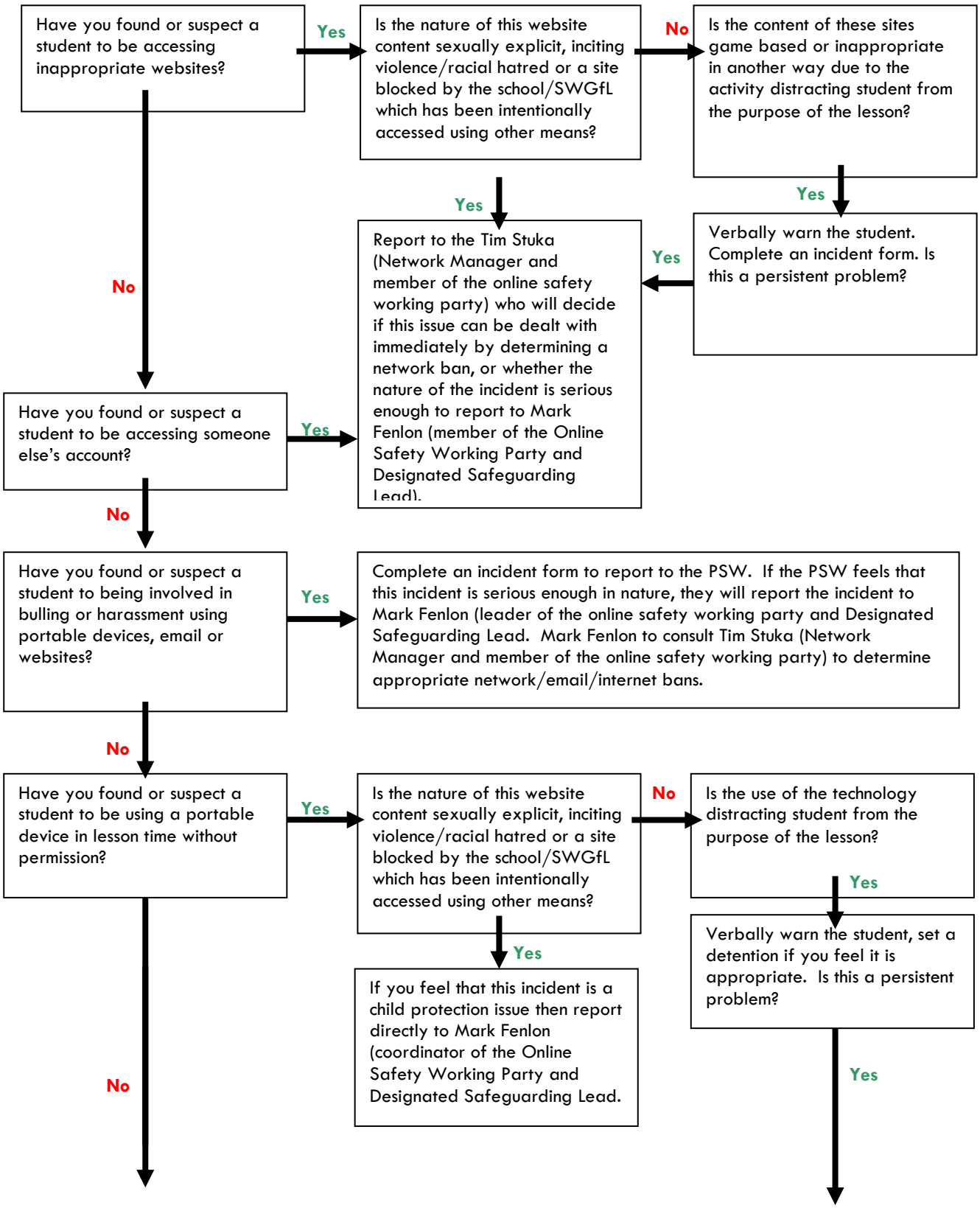
If any apparent or actual misuse appears to involve illegal activity (i.e. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material, other criminal conduct or materials) the flow chart below shows the process which is put into practice.

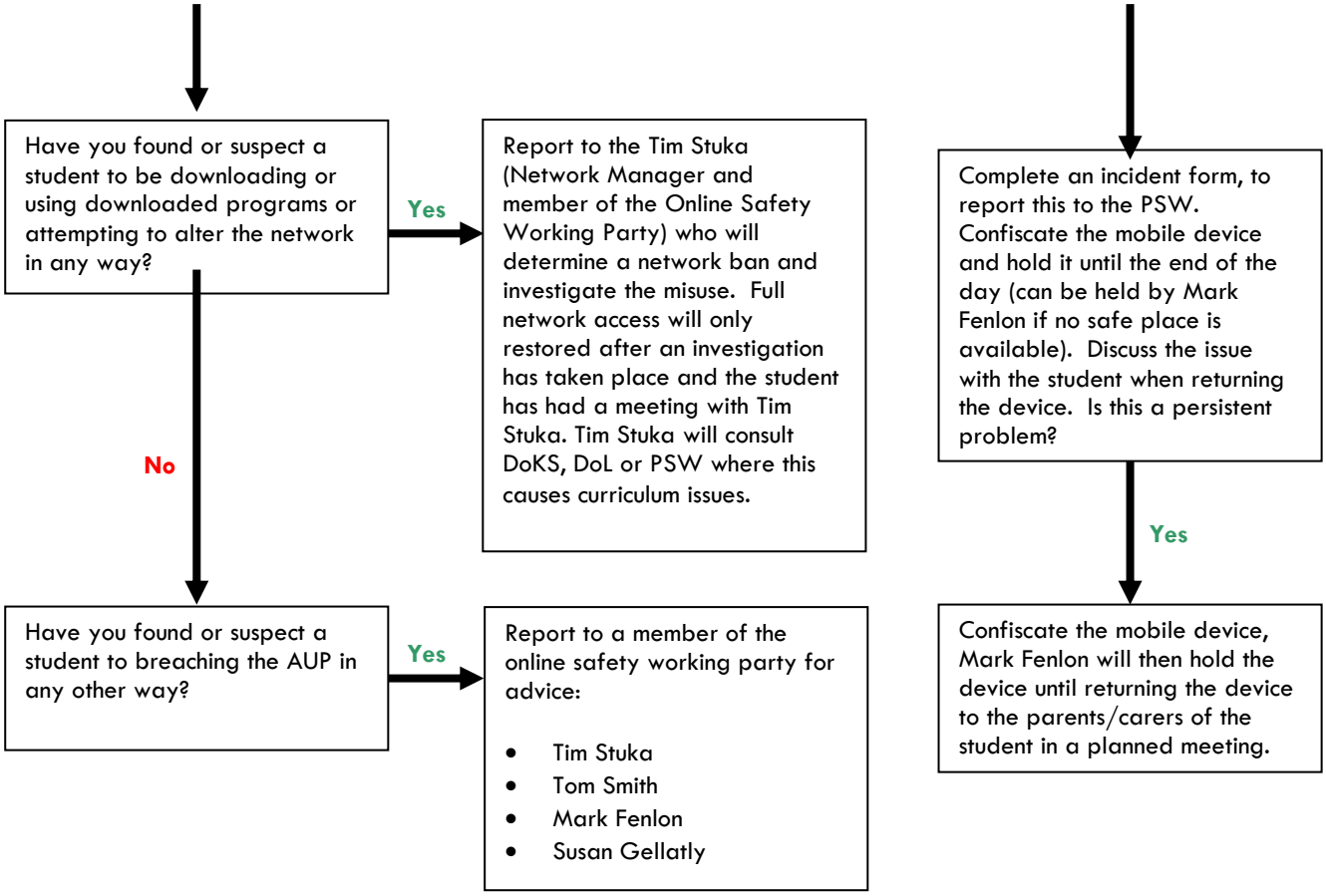


If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet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

Inappropriate activity

In the most likely scenario, teachers will need to deal with incidents that involve inappropriate rather than illegal misuse by students. It is important that any incidents are dealt with as soon as possible and in an appropriate 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; a guide to this process is shown below:




Have you found or suspect a student to be downloading or using downloaded programs or attempting to alter the network in any way?
Yes
Report to the Tim Stuka (Network Manager and member of the Online Safety Working Party) who will determine a network ban and investigate the misuse. Full network access will only restored after an investigation has taken place and the student has had a meeting with Tim Stuka. Tim Stuka will consult DoKS, DoL or PSW where this causes curriculum issues.
Complete an incident form, to report this to the PSW. Confiscate the mobile device and hold it until the end of the day (can be held by Mark Fenlon if no safe place is available). Discuss the issue with the student when returning the device. Is this a persistent problem?
Yes
Confiscate the mobile device, Mark Fenlon will then hold the device until returning the device to the parents/carers of the student in a planned meeting.
No
Have you found or suspect a student to breaching the AUP in any other way?
Yes
Report to a member of the online safety working party for advice:
Tim Stuka
Tom Smith
Mark Fenlon
Susan Gellatly

Students Actions/Sanctions

Incidents:	Refer to the supervising class teacher to that ensure they are aware.	Refer to the relevant Director of Learning	Refer to Online Safety working Party	Refer to Police	Refer to technical support staff for filtering	Head of Year or PSW Inform parents/carers	Removal of network/internet access	Verbal warning	Further sanction eg detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal.	☑		☑	☑	☑	☑	☑		☑
Unauthorised use of non-educational sites during lessons	☑	☑					☑	☑	
Unauthorised use of mobile phone / digital camera / other handheld device	☑	☑						☑	
Unauthorised use of social networking / instant messaging / personal email	☑	☑	☑		☑	☑	☑	☑	☑
Unauthorised downloading or uploading of files	☑	☑	☑		☑	☑	☑	☑	☑
Allowing others to access school network by sharing username and passwords			☑				☑	☑	☑
Attempting to access or accessing the school network, using another student's / pupil's account			☑				☑	☑	☑
Attempting to access or accessing the school network, using the account of a member of staff			☑				☑	☑	☑
Corrupting or destroying the data of other users			☑				☑	☑	☑

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑		☑			☑	☑	☑	☑
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			☑			☑	☑	☑	☑
Using proxy sites or other means to subvert the school's filtering system	☑		☑			☑	☑	☑	☑
Accidentally accessing offensive or pornographic material and failing to report the incident	☑							☑	
Deliberately accessing or trying to access offensive or pornographic material	☑	☑	☑		☑	☑	☑	☑	☑
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☑	☑						☑	

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Principal	Refer to Local Authority	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**.	☑	☑	☑	☑	☑	☑	☑	☑
Excessive or inappropriate but otherwise legal personal use of the internet/social networking sites/instant messaging/personal email.	☑	☑				☑		☑
Unauthorised downloading or uploading of files	☑	☑			☑	☑		☑
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	☑	☑			☑	☑		☑
Careless use of personal data eg holding or transferring data in an insecure manner	☑					☑		
Deliberate actions to breach data protection or network security rules	☑	☑	☑	☑	☑	☑	☑	☑
Corrupting or destroying the data of other users or causing **deliberate damage** to hardware or software	☑	☑			☑	☑	☑	☑
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑	☑				☑		☑
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications **with students**	☑	☑				☑		☑
Actions which could compromise the staff member's professional standing	☑	☑				☑		☑
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☑	☑				☑		☑

Using proxy sites or other means to subvert the school's filtering system	☑	☑			☑	☑		☑
Accidentally accessing offensive or pornographic material and failing to report the incident	☑				☑	☑		
Deliberately accessing or trying to access offensive or pornographic material	☑	☑	☑	☑	☑	☑	☑	☑
Breaching copyright or licensing regulations	☑					☑		
Continued infringements of the above, following previous warnings or sanctions	☑	☑	☑			☑	☑	☑

Linked policies

- **CSIA Bring Your Own Device Wireless Policy (BYOD)** –Describes what devices can connect to the BYOD network and how they should be used to support learning for VI Form students.
- **Student Acceptable Use Policy (Student AUP)** - Describes the services offered to students and acceptable uses of the school network, Internet access and email.
- **Staff Acceptable Use Policy (Staff AUP)** - Describes the services offered to staff and acceptable uses of the school network, Internet access and email.
- **Social Media Policy** - This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.