SIDMOUTH COLLEGE

Online Safety Policy

Policy adopted by the Resources Committee: 1st December 2020

believe • inspire • succeed

Policy last approved: **February 2016 (FGB)**

Policy review date: **December 2022**

Contents

Introduction

This Online Safety policy document considers all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies.

National guidance suggests that it is essential for schools to take a leading role in online safety. The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering online safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Sidmouth College has made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, through our Online Safety policy, we will ensure that the college meets its statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the College's protection from legal challenge, relating to the use of ICT.

This policy should be read in conjunction with the following policies:

- ***Data and Information Security Policy***
- ***Data Protection Policy***
- ***Filtering Policy***
- ***Staff and Visitor Acceptable Use Policy***
- ***Student Acceptable Use Policy***

Background / Rationale

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. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

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 (e.g. behaviour, 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 a committee made up of:

- School Online safety Coordinator
- Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff

Schedule for Development / Monitoring / Review

This online safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*December 2020*
The implementation of this online safety policy will be monitored by the:	Online safety Coordinator / Committee, and the Senior Leadership Team
Monitoring will take place at regular intervals:	*Summer Term*
The Governing will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Summer Term
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:	Summer Term
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Safeguarding Staff (CC), Police and Appropriate External Agencies.

The school will monitor the impact of the policy using:

- Logs of reported incidents (SIMS, CPOMS, Boost)
- Sophos monitoring logs of internet activity
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students (e.g. Ofsted “Tell-us” survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

Scope of the Policy

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

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 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 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 roles and responsibilities for online safety of individuals and groups within the College:

Principal and Senior Leaders:

- The Principal is responsible for ensuring the safety (including online safety) of members of the College community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Principal / Senior Leaders are responsible for ensuring that the Online safety Coordinator / Officer 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 Senior Leadership Team will receive regular monitoring reports from the Online safety Co-ordinator / Officer.
- 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 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)

Governors:

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 receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body is responsible for the role Online Safety Governor.

The role of the Online Safety Governor includes:

- Regular meetings with the Online Safety Co-ordinator
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors and the FGB.

Online Safety Coordinator:

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the College 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
- liaises with College ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- reports to Senior Leadership Team

Network Manager:

The Network Manager is responsible for ensuring:

- that the College's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the College meets the online safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- that users may only access the College's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the College's filtering policy, is applied and updated on a regular basis.
- that he / she keeps 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in College policies

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current College online safety policy and practices
- they have read, understood and signed the College Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online safety Co-ordinator for investigation / action / sanction
- digital communications with students (email / voice) should be on a professional level and only carried out using official College systems
- online safety issues are embedded in all aspects of the curriculum and other College activities
- students understand and follow the College online safety and acceptable use policy
- students 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 College activities
- 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 College 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

Designated Child Protection Officer:
Should be trained in online 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

Online safety Committee:
Members of the Online safety committee will assist the *Online safety Coordinator* with:

- the production / review / monitoring of the College online safety policy / documents.

Students:

- are responsible for using the College ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to College 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 College policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand College 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 College and realise that the College's Online safety Policy covers their actions out of College, if related to their membership of the College

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 College will therefore take every opportunity to help parents understand these issues through, newsletters, letters, website 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 College website / on-line student records in accordance with the relevant College Acceptable Use Policy.

Visitors:
Visitors who access College ICT systems as part of the Extended College provision will be expected to agree to the staff / visitor AUP before being provided with access to College 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 College's online safety provision. Children and young people need the help and support of the College to recognise and avoid online safety risks and build their resilience.

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of Computer Studies / PHSE and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College
- 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 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 College
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

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

- *Letters*
- *Newsletters*
- *Web site*

Education & Training – Staff

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. 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 College online safety policy and Acceptable Use Policies
- The Online safety Coordinator will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing current guidance documents.
- This Online safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online safety Coordinator will provide advice / guidance / training as required to individuals as required

Training – Governors

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

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

Technical – infrastructure / equipment, filtering and monitoring

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

- College ICT systems will be managed in ways that ensure that the College meets the online safety technical requirements outlined in the Online safety / Data Security 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 College ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to College ICT systems. *Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed annually, by the Online safety Committee.*
- All users will be provided with a username and password by the ICT department. The Network Manager *will keep an up to date record of users and their usernames. Users will be required to change their password every 50 days.*
- The "master / administrator" passwords for the College ICT system, used by the Network Manager must also be available to the Principal or other nominated senior leader and kept in a secure place.
- 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.
- The College maintains and supports the managed filtering service provided by Sophos.
- The College has provided enhanced user-level filtering through the use of the Sophos filtering programme.
- In the event of the Network Manager 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.
- Any filtering issues should be reported immediately to the College Network Manager and SLT.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online safety Committee
- College ICT technical staff regularly monitor and record the activity of users on the College 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 'SWGfL Whisper' / Confide for users to report any actual / potential online safety incident to the Online safety Committee.
- 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 College systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the College system.

- An agreed policy is in place that forbids staff from installing programmes on College workstations.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on College workstations / portable devices.
- The College infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.

Curriculum

Online safety should be 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, 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, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the 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.
- 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.

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 College 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.
- Staff are allowed to take digital / video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should only be taken on College 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 College into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students'' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the College website (this is covered as part of the photographic consent form signed by parents or carers at the start of the year)

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) which states that personal data must be:

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

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- 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
- the device must be password protected (many memory sticks / cards and other mobile devices cannot 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 College policy (below) 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 College currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to College	x				x			
Use of mobile phones in lessons		x						x
Use of mobile phones in social time		x						x
Taking photos on mobile phones or other camera devices				x				x
Use of hand held devices e.g. PDAs, PSPs								x
Use of personal email addresses in College, or on College network	x					x		
Use of College email for personal emails				x				x
Use of chat rooms / facilities				x				X
Use of instant messaging ** Microsoft Lync IMs are allowed.*				x*				x*
Use of social networking sites				x				x
Use of blogs				x				X

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

- The official College email service may be regarded as safe and secure and is monitored. *Staff and students should therefore use only the College email service to communicate with others when in College, or on College systems (e.g. by remote access).*
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the College 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 students or parents / carers (email, chat, etc.) must be professional in tone and content. *These communications may only take place on official (monitored) College systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.*
- Students will be provided with individual College email addresses for educational use.

- Students 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 College website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

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

		Acceptable	Acceptable at certain times	Nominated users only	Unacceptable	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, e.g. 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 College or brings the College into disrepute				X	
Using College systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the College					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 (e.g. 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 e.g. Youtube			X			

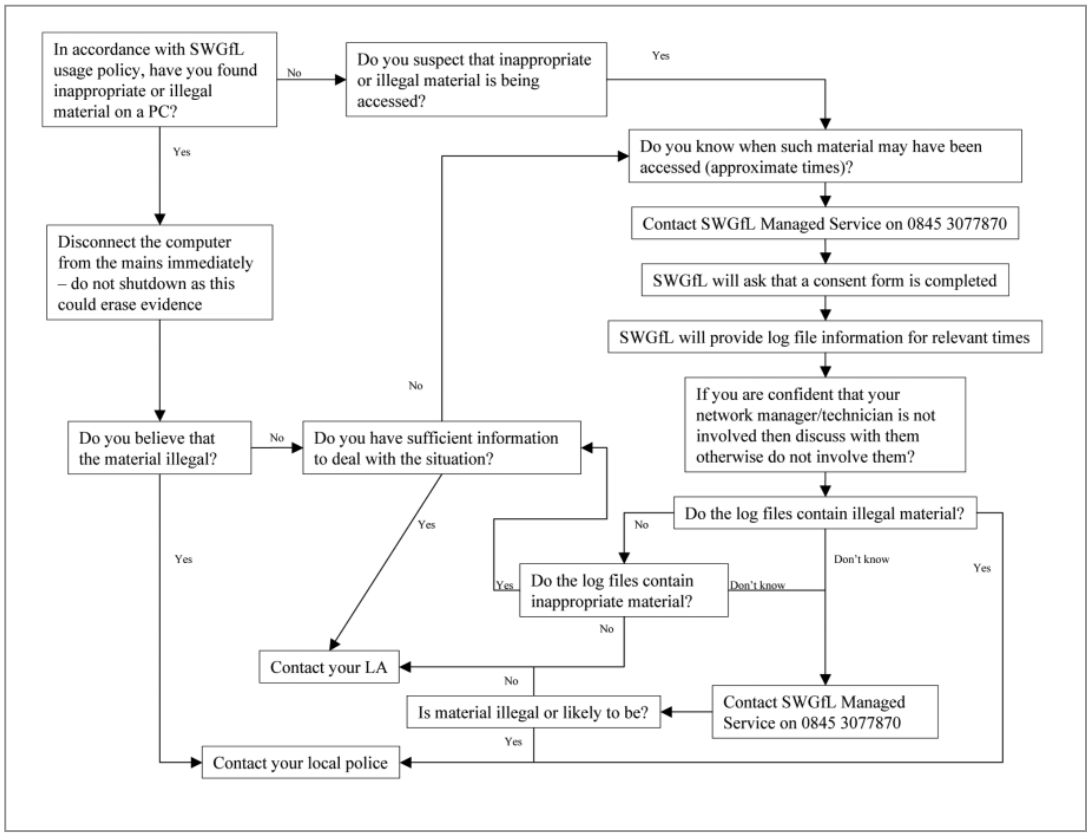
Responding to incidents of misuse

It is hoped that all members of the College 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

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



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.

It is more likely that the College 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 College 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

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of House / other	Refer to Principal	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x		x	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	x
Unauthorised use of social networking / instant messaging / personal email	x							x	x
Unauthorised downloading or uploading of files		x			x			x	x
Allowing others to access College network by sharing username and passwords		x			x				
Attempting to access or accessing the College network, using another student's 's account		x			x				
Attempting to access or accessing the College 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		x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x				x			x
Continued infringements of the above, following previous warnings or sanctions		x	x		x	x	x		x
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College			x		x	x	x		x
Using proxy sites or other means to subvert the College'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
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 line manager	Refer to Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Investigation	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	X	X	X
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person's account		X	X	X	X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X			
Deliberate actions to breach data protection or network security rules		X	X		X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students		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 College into disrepute or breach the integrity of the ethos of the College	X	X			X	X	X	X
Using proxy sites or other means to subvert the College's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Breaching copyright or licensing regulations		X	X		X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X		X		X	X

Appendices

Can be found in the following section:

- Legislation
- Glossary of terms

Legislation

Users should be aware of the legislative framework under which this Online safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

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

Computer Misuse Act
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
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.

GDPR
The General Data Protection Regulations provides a set of principles which govern how the College handles personal data. In summary, these principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary for the purpose it was processed
- Accurate and where necessary kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security of the data

Freedom of Information Act
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
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
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
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 College reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act
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
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
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
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
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
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
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 a 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
The new 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, connexions 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
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
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act
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 College 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 College 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
Empowers Principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Glossary of terms

AUP	Acceptable Use Policy – 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
GDPR	General Data Protection Regulations
ICT	Information and Communications Technology
INSET	In Service Education and Training
LA	Local Authority
LSCB	Local Safeguarding Children Board
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SEF	Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SWGfL	South West Grid for Learning – 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.