ONLINE SAFEGUARDING POLICY

Schedule for Development / Monitoring / Review

This Online Safeguarding policy was approved by the Governing Committee on:	*Spring 2020*
Review cycle	*Annual*
Next review date	*Sept 2025*
The implementation of this Online Safety policy will be monitored by the:	*Principal*
Monitoring will take place at regular intervals:	*Monitoring will take place across the academic year.*
The Governing Committee will receive a report on the implementation of the Online Safeguarding Policy (which will include anonymous details of online safety incidents) at regular intervals:	*The Directors will be updated 3 times a year within governor's meetings (or more frequently when necessary). Chair of Directors will sign any Online Safeguarding issues within these meetings.*
The Online Safeguarding 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 safeguarding or incidents that have taken place. The next anticipated review date will be:	*Summer each year and updated throughout the year in accordance with any updated national documentation.*
Should serious online safeguarding incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Academy Group Officials, LADO, Police*

Amendments/Review
Sept 2024 – Smoothwall implemented at TVS through which VC Rossendale access IT services. IT access on site at VC Blackpool is via Blackpool council. The IT Manager is currently in the process of obtaining Cyber essentials accreditation for TVS and VC to be completed by summer term 25. Blackpool council currently hold Cyber Essentials Plus accreditation.

The college will monitor the impact of the policy using:

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

Scope of the Policy

This policy is written to reflect the service level (SLA) agreement with Tor View School for the provision of technical services and the associated implementation and monitoring of filtering systems

Online Safeguarding must:
Protect and educate learners and staff in their use of technology, and have the appropriate mechanisms to intervene and support incidents where appropriate.

The breadth of issues classified within Online Safeguarding are considerable but can be categorised into three areas:

Content: Being exposed to illegal, inappropriate or harmful material.
Contact: Being subjected to harmful online interaction with other users.
Conduct: Personal online behaviour that increases the likelihood of, or causes, harm.

- This policy applies to all members of the college community (including staff, directors, learners, volunteers, advocates, visitors, community users) who have access to and are users of college digital technology systems, both in and out of the college / academy.

- The college will deal with such incidents within this policy and associated conduct and anti-bullying policies and will, where appropriate, inform advocates of incidents of inappropriate Online Safeguarding behaviour that take place out of college.

Roles and Responsibilities

It is everyone's responsibility to ensure policy and procedures are understood and respected by all at all times.

Directors
Directors are responsible for the approval of the Online Safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information about Online Safeguarding incidents and monitoring reports. A member of the Directors Committee has taken on the role of Safeguarding Governance including online safeguarding.

The role of the Online Safeguarding Director will include:

- Regular meetings with the Principal
- Regular monitoring of Online Safeguarding incident logs
- Regular monitoring of filtering / change control logs
- Reporting to the Director's committee.

Principal

- The Principal has a duty of care for ensuring the safety (including Online Safeguarding) of members of the college community.

- The Principal should be aware of the procedures to be followed in the event of a serious Online Safeguarding allegation being made against a member of staff.

- The Principal is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Network Manager / Technical staff
The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- That the college's / academy's technical infrastructure is secure and is not open to misuse or malicious attack

- That the college meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with Online Safeguarding technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in relevant policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of Online Safeguarding matters and of the current college Online Safeguarding Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Principal for investigation / action / sanction
- All digital communications with learners/advocates should be on a professional level and only carried out using official college systems
- Online Safeguarding issues are embedded in all aspects of the PACE curriculum and other activities.
- Learners understand and follow the Online Safeguarding Policy and acceptable use policies.
- Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. (Where appropriate)
- Learners monitor the use of digital technologies, mobile devices, cameras etc in lessons and other college activities (where allowed) and implement current policies with regard to these devices.

Designated Safeguarding Lead

Should be trained in Online Safeguarding issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with other adults
- Potential or actual incidents of grooming
- Online-bullying

(It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop)

Learners:

- Are responsible for using the college digital technology systems in accordance with the Learner Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (Where appropriate)

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Valley College encourage learners to tell a member of staff or another adult if they have any concerns.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- Should understand the importance of adopting good Online Safeguarding practice when using digital technologies out of college and realise that the college's / academy's Online Safeguarding Policy covers their actions out of college, if related to their membership of the college.

Valley College have representatives from within college that meet termly as a Learner Voice group. This group is facilitated by the Vice Principal and the Extended Services Lead to discuss issues and distribute information to their peers. During these meetings views can be taken from learners in relation to Online Safeguarding.

Advocates

Advocates play a crucial role in ensuring that their learners understand the need to use the internet / mobile devices in an appropriate way. The college will take every opportunity to help advocates understand these issues through Open Evenings, newsletters, letters, website / and information about relevant national / local online safety campaigns / literature.

Advocates will be encouraged to support the college in promoting good online safeguarding practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at college events
- Their learner's personal devices in the college (where this is allowed)

Valley College strive to ensure learners and advocates are kept up to date with the most recent changes in Online Safeguarding.

Education – Learners

- Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in Online Safeguarding / digital literacy is therefore an essential part of the college's / academy's Online Safeguarding provision. Learners who need the help and support of the college to recognise and avoid online safety risks and build their resilience will be supported to do so.
- Online Safeguarding should be a focus in all areas of college PACE and staff should reinforce Online Safeguarding messages where relevant.
- Online safeguarding should be provided as part of Computing / IAG and should be regularly revisited.
- Learners should be supported to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Learners should be supported to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Learners should be helped to understand the need for the Learner Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside college / academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

- In lessons where internet use is pre-planned, it is best practice that learners 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 learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites visited.
- It is accepted that from time to time, for good educational reasons, learners may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Advocates

As a college we will work with advocates when required to ensure their learners use technology safely and responsibly at home and at college and seek to provide information on potentially harmful and inappropriate material on the internet and how to respond when appropriate.

Education – The Wider Community

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

- The college website will provide online safeguarding information for the wider community

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safeguarding training will be made available to staff annually alongside safeguarding training. This will be regularly updated and reinforced.

- All new staff should receive online safeguarding training as part of their induction programme (Safeguarding Training) ensuring that they fully understand the Online Safeguarding Policy and Acceptable Use Agreements.

- It is expected that some staff will identify online safeguarding as a training need within the appraisal process.

- This Online Safeguarding Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

- The Designated Safeguarding Lead will provide advice / guidance / training to individuals as required.

Training – Directors

Directors take part in online safeguarding training / awareness sessions. This may be offered in a number of ways:

- Training through National College portal.

- Participation in college training / information sessions for staff.

Technical – infrastructure / equipment, filtering and monitoring

The college has a managed ICT service provided by an outside contractor via an SLA with Tor View School.

The college will ensure that it's infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- College technical systems will be managed in ways that ensure that the college meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of college technical systems via the SLA
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to technical systems and devices.
- The "master / administrator" passwords for the ICT systems, used by the Network Manager (or other person) are managed by Tor View as part of the SLA. (available to the Principal/Online Safeguarding Lead and kept in a secure place).
- The ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring should ensure that learners are safe from terrorist and extremist material when accessing the internet.
- The SLA has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users
- Technical staff regularly monitor and record the activity of users on the technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. Staff report this to the Technical Team/Principal.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the college systems and data. These are tested regularly. The college infrastructure and individual workstations are protected by up to date virus software.
- An agreed Community Acceptable Use Policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / learners / community users) and their advocates are allowed on college devices that forbids staff from downloading executable files and installing programmes on college devices.
- It is agreed that the use of removable media (eg memory sticks / CDs / DVDs) by users on college devices is not permitted. Personal data cannot be sent over the internet or taken off the college site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

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

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

The college choose to include these aspects of their policy in a comprehensive Acceptable Use Agreement, rather than in a separate Mobile Technologies Policy. It is suggested that the college should in this overall policy document, outline the main points from their agreed policy.

The college Acceptable Use Agreements for staff, learners and advocates will give consideration to the use of mobile technologies

	College Devices			Personal Devices		
	College owned for single user	**College owned for multiple users**	**Authorised device[1]**	**Learner owned**	**Staff owned**	**Visitor owned**
Allowed in college	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only (Filtered)	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*

Personal devices:

- All visitors are asked to turn off their mobile phones before entering the building and sign an acceptable use policy when they sign in. No audio or visual recording of meetings within college are permitted.
- All staff are allocated lockers for their personal belongings, which includes mobile phones.
- All learner mobile phones are stored in allocated lockers with personal belongings during the college hours.
- Staff have access to a college mobile phone for work experience use.
- The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The 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 learners about the risks associated with the taking, using, sharing and the publication and distribution of images. In

Within Valley College, it is age appropriate to allow appropriate use of mobile phones during unstructured times. The learners and advocates (where relevant) are required to sign an acceptable use policy should they wish to use their device and this may be supervised and monitored by staff.

particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from learners and/or advocates (when relevant) will be obtained before photographs of learners are published on the college website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, advocates are welcome to take videos and digital images of their learner at college events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should advocates comment on any activities involving other learners in the digital / video images.
- Staff and volunteers 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 learners are appropriately dressed and are not participating in activities that might bring the individuals or the college / academy into disrepute.
- Learners must not take, use, share, publish or distribute images of others without the consent of those involved.
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Learner's work can only be published with the permission of the learner and/or advocate (as relevant).

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The college / academy must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO). The college / academy may also wish to appoint a Data Manager and systems controllers to support the DPO.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice. (see Privacy Notice section in the appendix)
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.

(See Freedom of Information Policy which sets out how it will deal with FOI requests.)

- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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, memory stick or any other removable media:

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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the college / academy considers the following as good practice:

- The official college email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and learners 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 must immediately report, to the nominated person – in accordance with the college policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and learners or advocates (email, social media, chat, blogs, VLE 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 social media must not be used for these communications.
- Learners should be taught about Online Safeguarding issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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

College staff should ensure that:

- No reference should be made in social media to learners, advocates or college staff
- They do not engage in online discussion on personal matters relating to members of the college community
- Personal opinions should not be attributed to the college /local authority / MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Official college social media accounts i.e. Facebook have:

- A clear process for the administration and monitoring of the account – involving at least two members of staff (Vice Principal/IT support/ Admin Lead)
- A code of behaviour for users of the account
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under college / academy disciplinary procedures

Personal Use:

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

Monitoring of Public Social Media

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

The college's use of social media for professional purposes will be checked regularly by the Principal to ensure compliance with the college policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from college and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a college context eg the nature of those 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 / or outside the college when using college equipment or systems. The college policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute				X	
Using college systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			x			
On-line gaming (non-educational)					x	
On-line gambling					x	

On-line shopping / commerce				x	
File sharing					x
Use of social media				x	
Use of messaging apps				x	
Use of video broadcasting e.g. Youtube		x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Principal/DSL and report immediately to the police.

Other Incidents

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

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

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

- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

College Actions & Sanctions

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:

Learner Incidents	Refer to teacher/tutor	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform advocates (as applicable)	Removal of network / internet access	Warning	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x					
Unauthorised use of non-educational sites during college learning session	x			x				
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	x		x				
Unauthorised / inappropriate use of social media / messaging apps / personal email	x							
Unauthorised downloading or uploading of files	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 learners' password		x		x		x		

Attempting to access or accessing the college / academy network, using the account of a member of staff	x	x		x		x		
Corrupting or destroying the data of other users		x		x		x		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x		x	x	x		
Continued infringements of the above, following previous warnings or sanctions		x		x	x		x	
Actions which could bring the college / academy into disrepute or breach the integrity of the ethos of the college		x						
Using proxy sites or other means to subvert the college's / academy'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		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x	x		x		

Staff Incidents	Refer to Local Authority /HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X				
Inappropriate personal use of the internet / social media / personal email			x	x		
Unauthorised downloading or uploading of files	x	x	x	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
Careless use of personal data e.g. holding or transferring data in an insecure manner	x		x	x	x	x

Deliberate actions to breach data protection or network security rules			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
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x	x	x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with learners	X	X	X	X	X	x
Actions which could compromise the staff member's professional standing			X	X	X	x
Actions which could bring the college / academy into disrepute or breach the integrity of the ethos of the college / academy			X	X	X	x
Using proxy sites or other means to subvert the college's / academy's filtering system			X	X	X	x
Accidentally accessing offensive or pornographic material and failing to report the incident			x	x		
Deliberately accessing or trying to access offensive or pornographic material			X	X	X	x
Breaching copyright or licensing regulations	X	X	X	X	X	x
Continued infringements of the above, following previous warnings or sanctions	X		X	X	X	x

Acknowledgements

Copyright of this template policy is held by SWGfL. Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development.