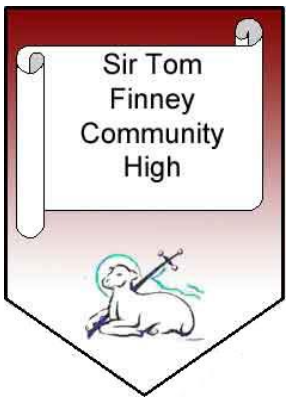


Sir Tom Finney Community High School

Online-Safety Policy
January 2019

Development / Monitoring / Review of this Policy

This online-safety policy has been developed by a working group made up of:

Headteacher (DSL2), Computing curriculum co-ordinator, Network manager, representatives from teachers/teaching assistants, Governor representation, student representation

Schedule for Development / Monitoring / Review

The policy ratified by *Governors Curriculum Committee:*	committee meetings spring 2019
The implementation of this policy will be monitored by the:	*Working group / Coordinator / governing body*
Monitoring will take place at regular intervals:	*Online safety group meetings, half termly*
The *Curriculum Committee* will receive a report on the implementation of the policy generated by the monitoring group at regular intervals:	*Annually*
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats or incidents that have taken place. The next anticipated review date will be:	*Spring 2020*
Should serious incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:

- reported incidents
- Monitoring of internet activity
- Internal monitoring data for network activity

Plus, additional informal monitoring by network manager and all staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are also 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 incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data and to report this to appropriate external sources eg Police.

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 behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school

Governors:

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

- *attending and participating in relevant monitoring group*
- *reporting to Governors meeting*

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the co-ordinator, senior staff and network manager; however it is clear that this is a whole school responsibility and as such all school staff maintain a responsibility to be diligent and vigilant and follow procedures and codes of conduct appropriately.
- The Headteacher and Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to support those in school who carry out the 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 / Senior Management Team will receive monitoring reports.

Head, Co-ordinator, Safeguarding/Child Protection DSL, Network Manager and DPO:

HAVE A ROLE TO PLAY:

- the online safety working group
- a day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school policies / documents
- ensuring all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- providing training and advice for staff
- liaison with the Local Authority / relevant body
- liaison with school staff
- receiving reports of online safety incidents and creates a log of incidents to inform future developments
- informing and reporting to governors
- informing and reporting to Senior Leadership Team

Network Management:

have, as much as is possible, a responsibility for ensuring:

- that the school's infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required technical requirements and any 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
- that they keep up to date with online safety technical information in order to effectively carry out their role and to inform and update others as relevant
- that the use of the *network* is regularly monitored in order that any misuse / attempted misuse can be reported appropriately
- that monitoring software / systems are implemented and updated as appropriate

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher/DSP/Coordinator/network manager for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the online safety and acceptable use policies
- students have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations where appropriate in line with the cognitively ability of the student
- they monitor the use of digital technologies, mobile devices, cameras smart watches etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person /DPO

should be trained in online safety issues and be aware of the potential for child protection / safeguarding issues and/or GDPR 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

(note: it is important to emphasise that these are child protection and data protection issues, not technical issues, simply that the technology provides additional means for issues to develop.)

Online Safety Group

provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Group will assist with:

- the production / review / monitoring of the school online safety policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incidents as relevant
- consulting stakeholders about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- where able 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, through appropriate teaching and learning at differentiated levels, the safe use of mobile devices and digital cameras. They should also know and understand the rules about 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 Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems will be expected to have read and understood a Community User AUA before being provided with access to school systems.

Policy Statements

Education – students / pupils

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. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- **A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons**
- **Key messages should be reinforced as part of assemblies and tutorial / pastoral activities**
- **Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school**
- **Staff should act as good role models in their use of digital technologies, the internet and mobile devices**
- **in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.**
- **Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.**
- **It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that those sites are temporarily removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.**

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/

Education – The Wider Community

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

- Providing courses in use of new digital technologies, digital literacy and online safety as part of adult learning and lettings
- Online safety messages targeted towards other relatives as well as parents.

- The school website could be used to provide online safety information for the wider community

Education & Training – Staff / Volunteers

All staff receive online safety guidance and understand their responsibilities, as outlined in this policy. Possible training requirements may be offered as follows:

- Online safety information via safeguarding training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive the above as part of their induction programme, ensuring that they fully understand the school policy and Acceptable Use Agreements.
- The Coordinator / DSP will receive regular updates through attendance at external events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to staff once ratified by Governors
- The Coordinator / DSP will provide advice / guidance to individuals as required.

Training – Governors / Directors

Governors should take part in awareness sessions by

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

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 procedures approved within this policy are implemented. It will also need to ensure that the relevant people will be effective in carrying out their responsibilities.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password; an up to date record of users and their usernames will be kept by the Network Manager. Users are responsible for the security of their username and password and are encouraged to change their password at regular intervals
- The “administrator” passwords for the school ICT system, must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- Network 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. 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.
- The school has provided differentiated user-level filtering
- The Network manager regularly monitors and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.

- 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 school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreement is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Agreement is in place that forbids staff from downloading executable files and installing programmes on school devices without prior knowledge of responsible persons.
- The use of removable media (eg memory sticks) is not allowed. CDs / DVDs by users on school devices must seek prior agreement

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- Parents/Carers must adhere to school policy and guidance from the Information Commissioner's Office, with regard to taking videos and digital images of their children at school events for their own personal use. 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 parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow 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, on school's facebook 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 digitally, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published
- Student's work can only be published with the permission of the student

General Data Protection Regulations

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (May 2018) ; 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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

The school must ensure that it follows GDPR regulation and guidance including:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- A responsible person is identified as Data Protection Officer (DPO)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

Personal data should not be stored on portable computer systems, memory stick or any other removable media:

Communications

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. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. **Personal email addresses, text messaging or social media must not be used for these communications.**
- Students will be provided with individual school email addresses for educational use.
- Students will be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- acceptable user agreements; information and guidance on social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment

School staff should ensure that:

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

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg 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 school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the table would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems.

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

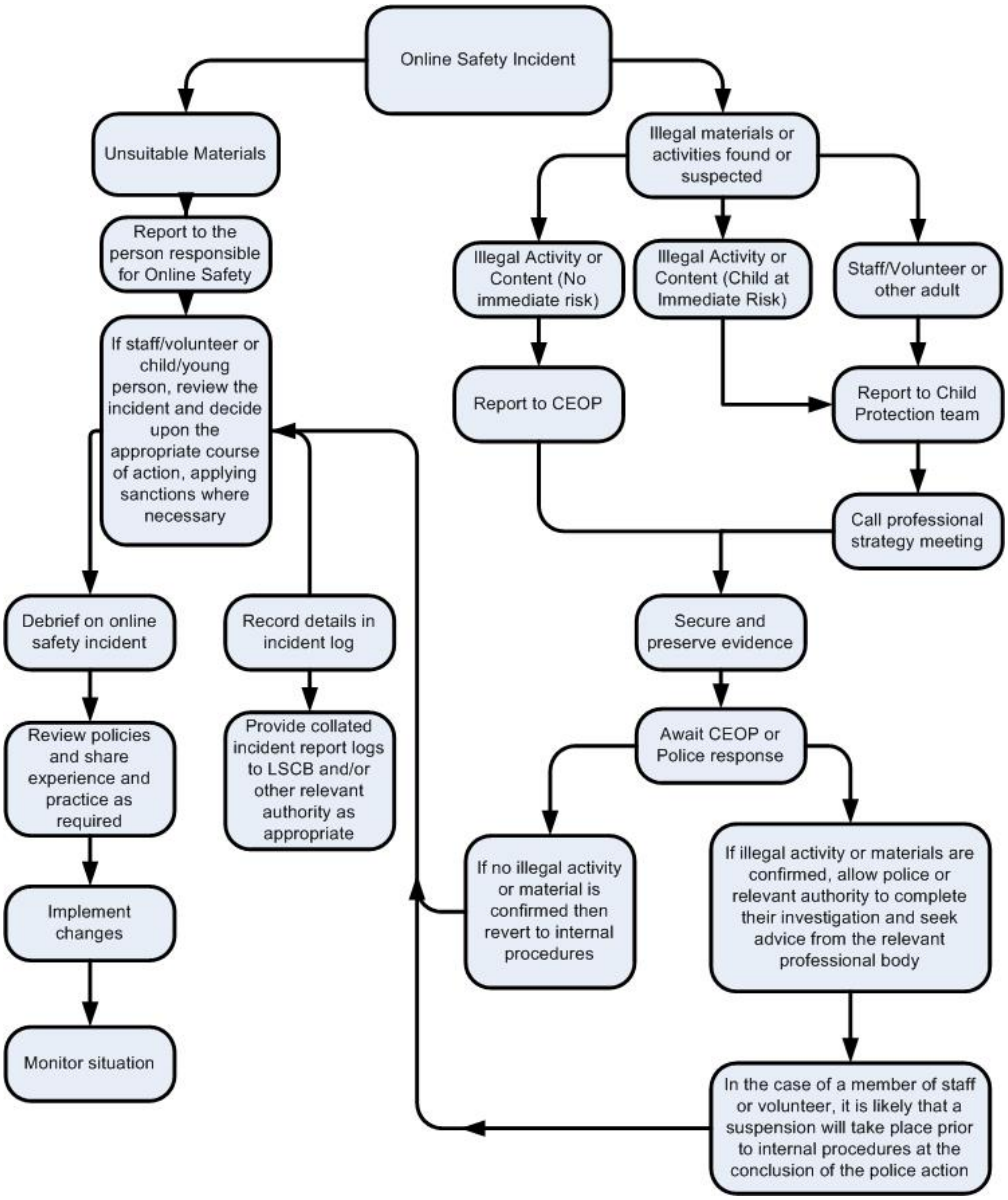
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection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

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the

machine being used for investigation. These may be printed, signed and attached (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated a judgement whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority 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
  - 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 school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed reference notes or forms should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Acknowledgements

- Members of the SWGfL
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication/update