Cape Cornwall School
Online Safety (E-Safety) Policy

Dream, Believe, Persevere, Achieve

Dissemination: Website and O Drive

Date policy approved by Governors: 18 March 2021 (Full Governing Body)

Date policy becomes effective: Immediately

Review date: UNDER REVIEW

Person responsible for Implementation and Monitoring: Headteacher, Designated Safeguarding Lead

Links to other relevant policies: GDPR, Safeguarding, Anti-Bullying, ICT Acceptable Use, Banned Substances, Student Behaviour, Disciplinary.

Scope of the Policy

This policy applies to all members of school (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's digital technology 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 off the school site and to impose sanctions for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to searching for, and screening, electronic devices and with regards to the deletion of data. In the case of both Acts, action can be taken over issues covered by the school's Behaviour Policy.

The school will manage incidents within this policy using the associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the school's Online Safety policy and for reviewing the effectiveness of the policy on a regular basis. This monitoring will be carried out by the

Governing Body receiving regular (termly) information about online safety incidents and monitoring reports, as a routine part of the monitoring of safeguarding. A member of the Governing Body has taken on the role of Safeguarding Governor, which will include :

- regular meetings with the Online Safety Lead (DSL) to review the implementation of this policy and any issues identified with regards to members of the school community;
- reporting to relevant Governors' meetings.

Head of School and Senior Leaders

- The Head of School has a duty of care for ensuring the safety (including online safety) of members of the school community. The day to day responsibility for online safety will be delegated to the DSL.
- The Head of School, Leadership Team member (Pastoral) and Designated Safeguarding Lead 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 procedures);
- The Head of School and Senior Leaders are responsible for ensuring that the DSL 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 Head of School will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles, as part of regular safeguarding meetings and, where appropriate, supervision.
- The Senior Leadership Team will receive regular monitoring reports from the DSL and will be informed of any significant breach of this policy.

Online Safety Lead (DSL)

 The Online Safety Lead will be the Designated Safeguarding Lead. The DSL:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school's 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/Trust/relevant body;
- liaises with IT technical staff;
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments via My Concern;
- meets regularly with the Safeguarding Governor to discuss current issues, review incidents and the implementation of this policy;
- provides relevant reports about online safety incidents for Governors.
- reports regularly to Senior Leadership Team.

They are aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data;

- access to illegal/inappropriate materials inappropriate online contact with adults/strangers; - potential or actual incidents of grooming;
- online-bullying

Network Manager/Technical staff

Those with technical responsibilities (TPAT IT) are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required online safety technical requirements and any Trust online safety policy/guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy;
- that 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 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 networks/internet/and digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Senior Leadership Team/DSL for investigation/action/sanction;
- that monitoring software and systems are implemented and updated as agreed to ensure their effectiveness.

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's Online Safety policy and practices;
- they have read, understood and signed the Staff Acceptable Use policy (AUP);
- they report any suspected misuse or problem to the Senior Leadership Team and/or DSL for investigation/action/sanction;
- all digital communications with students/parents/carers are on a professional level and only carried out using official school systems;
- online safety issues are embedded where appropriate in all aspects of the curriculum and other activities;
- students understand and follow the Online Safety policy and Acceptable Use policies;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras, 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.

Students:

- are responsible for using the school's digital technology systems in accordance with the student acceptable use agreement;
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand the school's policies on the taking/use of images and on online bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety policy covers their actions out of school, if related to their membership of the school.

Parents/carers

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 through parents' evenings, newsletters, letters, website, social media and information about national/local online safety literature. 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;
- access to parents' sections of the website, school social media and online student records.

Community Users and Visitors

Community users and visitors who access school systems or programmes as part of the wider school provision will be expected to sign an AUP before being provided with access to school 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 and digital literacy 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 where appropriate and staff should reinforce online safety messages across the curriculum. The online safety curriculum is planned to be broad, relevant and provide progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing and PSHE lessons and our tutorial programme and is regularly revisited:

- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities;
- Students are taught in all lessons to be critically aware of the materials and content they access online and are guided to validate the accuracy of information;
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;

- Students are 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;
- Students are 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 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 are 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 are 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 technical staff 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 – Parents/Carers

Many parents and carers may 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 and regulation of the children's online 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:

- Letters, newsletters, website;
- Parents/Carers evenings;
- High profile events/campaigns e.g. Safer Internet Day;
- Reference to the relevant websites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

From time to time the school may have 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 family learning courses in use of new digital technologies, digital literacy and online safety;
- Online safety messages targeted towards grandparents and other relatives as well as parents;
- The school website will provide online safety information for the wider community;
- Staff and students sharing their online safety expertise and good practice with other local schools;
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision.

Training – Staff

Staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual training for all staff updating on online safety, including this Online Safety policy and its updates;
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety policy and Acceptable Use Agreements;
- It is expected that some staff may identify online safety as a training need within the performance management process;
- The DSL will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations. These will be shared with staff as appropriate;
- The DSL will provide advice, guidance and training to individuals as required.

Training – Governors

Governors will take part in online safety training, alongside their safeguarding training, with particular importance for those who are members of any group involved in technology, online safety, health and safety and safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/Trust/National Governors Association/or other relevant organisation (e.g. SWGfL);
- Participation in school training and information sessions for staff or parents; - Training provided as part of Governors' Meetings.

Technical – infrastructure/equipment, filtering and monitoring

The school, as part of Truro and Penwith Academy Trust (TPAT) receives technical support from a central Trust IT Support Team. This team are aware of the technical requirements and policies of the school as well as local and national requirements and best practice for use of infrastructure, equipment, filtering and monitoring.

Use of digital and video images

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, 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 online bullying 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 potential 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;
- Written permission from parents or carers will be obtained before photographs of students are published on the school website, social media or in the local press;

- Staff and volunteers are allowed to take digital and 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. Students under the age of 12 are not usually considered to be able to give informed consent;
- 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 social media, particularly in association with photographs.
- Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation (see TPAT Data Protection (GDPR) Policy.

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 (e.g. by remote access);
- Users must immediately report 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. Such communication should be reported to the DSL;
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for students and staff. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the School or Trust liable to the injured party. Staff who act in such a way will face disciplinary action by the school. 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 students, staff and the school 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 (undertaken by TPAT)

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 Trust;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- Approval by the Head of School;
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
- A code of behaviour for users of the accounts, including:
      o Systems for reporting and dealing with abuse and misuse; o Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used by a member of staff the content must not refer to any school matter. It should be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy. Any communication which could result in reputational damage to the school will be considered under the disciplinary procedure.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively monitor the internet for public postings about the school;
- The school will effectively and appropriately respond to social media comments made by others according to a defined policy or process;
- The school's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from school IT systems. Other activities e.g. cyber-bullying is subject to school filtering and monitoring. Where identified, it could lead to disciplinary and/or legal action and/or involvement of the police and criminal prosecution. There are 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 following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –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 school or brings the school into disrepute			X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files				X

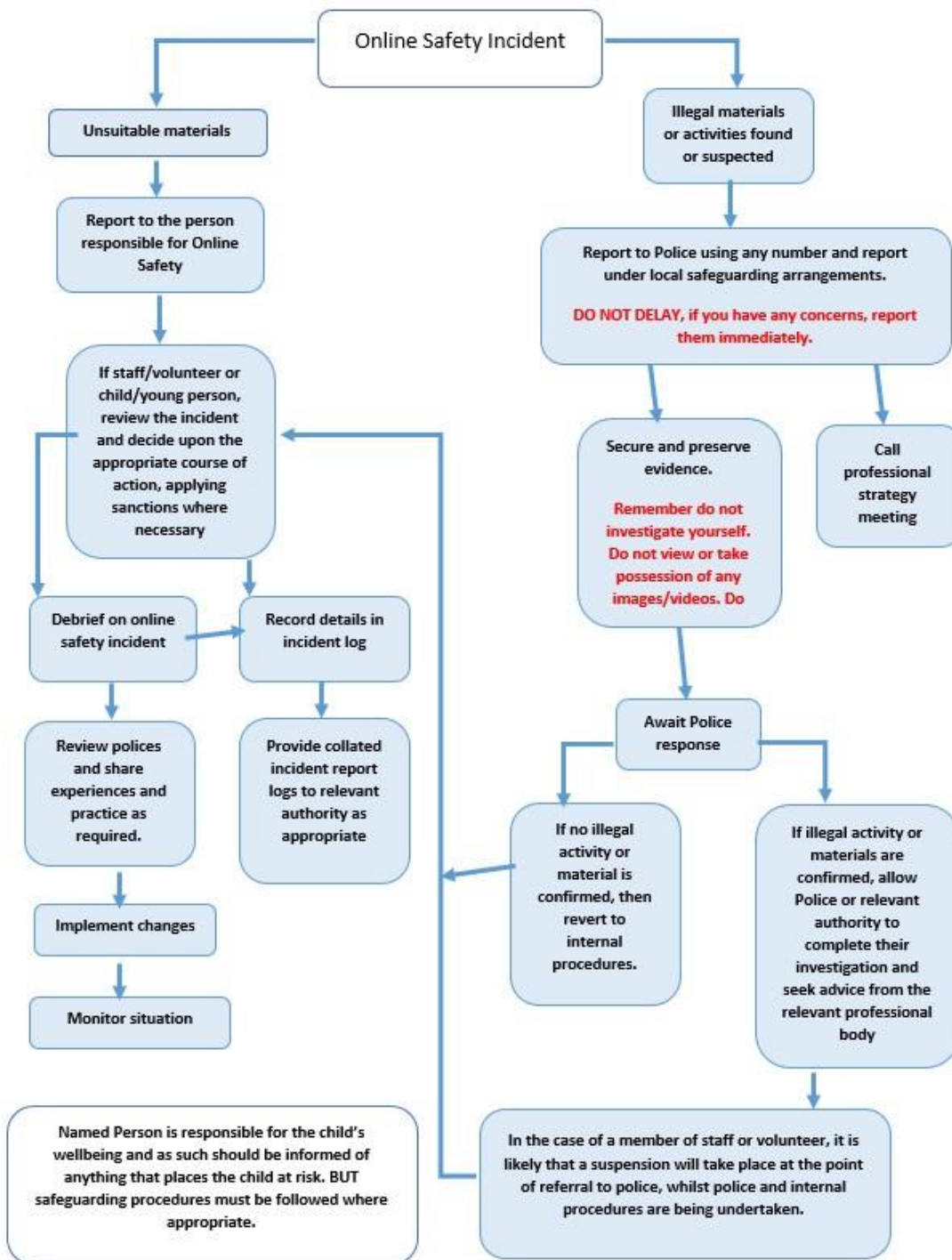|				
Revealing or publicising confidential or proprietary information (e.g. financial personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission)	/			
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X
Using school systems to run a private business				X
Infringing copyright				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 (see "User Actions" above).

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 right hand side of the flowchart below for responding to online safety incidents and report immediately to the police.

Online Safety Incident

Unsuitable materials

Illegal materials or activities found or suspected

Report to the person responsible for Online Safety

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

Implement changes

Monitor situation

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

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:

- At least two members of staff (including one senior leader) will be 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;
- 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:

  o   Internal response or disciplinary procedures; o Involvement of Trust or national/local organisations (as relevant); o 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:

  o   incidents of 'grooming' behaviour; o the sending of obscene materials to a child; o adult material which potentially breaches the Obscene Publications Act; o criminally racist material; o promotion of terrorism or extremism; o offences under the Computer Misuse Act (see User Actions chart above); o 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 safeguarding 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 linked to the relevant policies.