Online Safety Policy

Policy Name:	Online Safety Policy			Review Date: 14/03/2019	Every 3 Years 14/03/2022
Presented to the Resources Committee:	Date:14/03/2019	Adopted by the Full Governing Body:	Date:21/03/2019	Chair of Governors Signature:	

Scope of the policy

This policy applies to all members of the Queen's Park High School ('the school') community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of 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 empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy, the accompanying procedure as well as within the associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Misuse of the school's Online Safety Policy can damage the school's reputation and put members of the school at risk. Breach of this policy may lead to disciplinary action, and in serious cases, may be treated as gross misconduct leading to summary dismissal or suspension.

1. Roles and Responsibilities

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

Governors:

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy and accompanying procedures.

Headteacher and Senior Leaders:

- The Headteacher – Lyndsay Watterson - 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 Online Safety Co-ordinator Sarah Williams in her role as Safeguarding Lead.
- The Headteacher and Online Safety Co-ordinator 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 "Responding to incidents of misuse".
- The Headteacher is responsible for ensuring that the Online Safety Co-ordinator 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 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.

Online Safety Co-ordinator: Sarah Williams

- Is the Designated Safeguarding Lead
- leads the Online Safety group
- takes day to day responsibility for Online Safety issues and has a leading role In establishing and reviewing the School 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
- liaises with the Local Authority/relevant bodies
- liaises with school technical staff
- receives reports of Online Safety incidents and creates a log of incidents on CPOMS to inform future Online Safety developments

Network Manager/Technical staff: Dave Helsby

The Network Manager is responsible for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack
- the filtering is applied and updated on a regular basis – we also have the facility to block websites on a school basis.
- that the use of the network, internet and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Online Safety Co-ordinator for investigation.
- that monitoring systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

They are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current School Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy
- they have read, understood and signed the Data Protection Policy
- they report any suspected misuse or problems to the Headteacher or Online Safety Coordinator for investigation
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems, for example EduLink One
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety, Data Protection 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

Safeguarding Staff
They should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data and non-compliance with the General Data Protection Regulation (GDPR)
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

It is important to note that these are child protection issues, not technical issues; simply that the technology provides additional means for child protection issues to develop.

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 and information about national/local Online Safety campaigns/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 and on-line student records
- their children's personal devices in the school
- personal data in accordance with GDPR

Community Users/Lettings

Community Users who access school systems/website as part of the wider school provision will be expected to sign a user agreement before being provided with access to school systems.

2. Development/Monitoring/Review

The implementation of this Online Safety policy will be monitored by Sarah Williams – Online Safety Co-ordinator.

Should serious Online Safety incidents take place, the relevant external individuals and agencies will be informed (LA Safeguarding Officer/Police).

The School will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/students
    - parents/carers
    - staff

Online Safety Procedures

1. Training & Education

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the 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 is part of our computing and citizenship lessons and is regularly revisited
- Key Online Safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be 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 and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technician 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.

Parents/Carers

Some parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line 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, web site.
- Parents/Carers sessions
- High profile events/campaigns eg Safer Internet Day
- Reference to the relevant web sites/publications

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:

- Online Safety messages targeted towards other relatives as well as parents
- The school website will provide Online Safety information for the wider community
- Supporting feeder primary schools to enhance their Online Safety provision

Staff/Volunteers

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

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates through attendance at external training events from LA and other relevant organisations and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings
- The Online Safety Group will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in Online Safety training/awareness sessions, with particular importance for those who have responsibility for technology/Online Safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

PREVENT

- All staff have completed training on the PREVENT agenda to ensure they are aware of the warning signs of radicalisation and how to deal with any issues that arise.

- All SLT members have attended PREVENT awareness training and an action plan has been created around PREVENT.

- The school computers are monitored weekly as part of the Online Safety routine and the PREVENT agenda key words are now flagged up as focus words.

2. Infrastructure / Equipment, Filtering and Monitoring

The School will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety 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
- Users will be provided with a username and secure password by IT Support, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password frequently as per the ICT Policy
- Dave Helsby, 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. Illegal content (for example: 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
- No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment. Student computer screens can be monitored by staff using software in ICT rooms. Filter reports will be sent to the Designated Safeguarding Person for scrutiny and followed up as appropriate.
- 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.

3. 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 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school 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 must not be published/made publicly

available on social networking sites, nor must parents/carers comment on any activities involving other *students/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, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers.
- Any taking and processing of digital and video images should comply with the School's Data Protection Policy and the GDPR.

4. Data Protection

The School intends to comply with its legal obligations under the Data Protection Act 2018 and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security.

Please refer to the School's Data Protection Policy and Privacy Policies for more detail on how personal data should be processed. These can be obtained from the school website.

5. Communications

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

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.*
- **Users must immediately report, to Mrs S Williams, Safeguarding Lead – in accordance with the school** 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 students or parents/carers (email, chat, 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.
- All children can email safely through their password protected access on the school website which is monitored.
- Students are 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/academy website and only official email addresses should be used to identify members of staff.

- When in school staff should normally only use their mobile phones in private areas such as the staffroom. Unless they have specific consent of the Headteacher then they should not have phones out in areas where children are present.

6. Social Media - Protecting Professional Identity (see separate guidance)

7. Safe Learning Environments

All schools and local authorities have a duty of care to provide a safe learning environment for students 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 age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity 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 students, staff and the school through:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessments, including legal risk
- limiting access to personal information in compliance with the GDPR

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.

The school's use of social media for professional purposes will be checked regularly to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

8. Cyberbullying Unsuitable / inappropriate 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 school or outside school when using school equipment or systems.

The school policy restricts usage as follows:

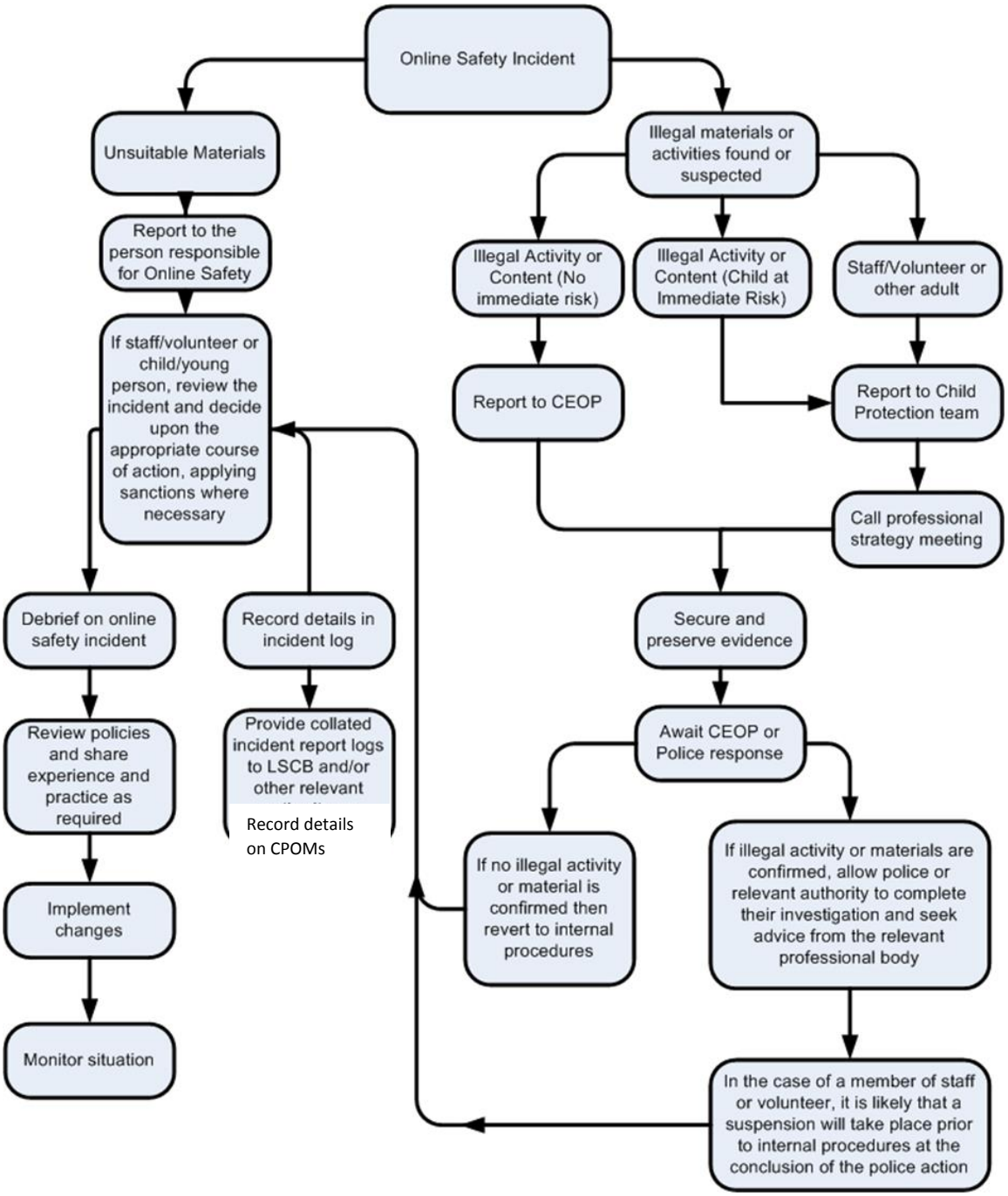
		Acceptable	*Acceptable at certain times*	*Acceptable for nominated user*	*Unacceptable*	*Unacceptable and illegal*
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008.					✓
	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.					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Threatening behaviour, including promotion of physical violence or mental harm				✓	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
	Using school systems to run a private business				✓	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				✓	
	Infringing copyright					✓
	Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)				✓	
	Creating or propagating computer viruses or other harmful files					✓
	Unfair usage (downloading/uploading large files that hinders others in their use of the Internet)				✓	
	On-line gaming (educational)		✓			
	On-line gaming (non-educational)				✓	
	On-line gambling				✓	
	Use of video broadcasting eg Youtube			✓		
	File sharing			✓		
	Use of social media & file sharing			✓		
	Use of messaging apps				✓	

9. 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 right hand side of the Flowchart (below and appendix) 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/volunteer 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 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
    - 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.
        - a report to the Data Protection Officer in accordance with the Data Protection Policy.

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 form should be retained by the group for evidence and reference purposes.