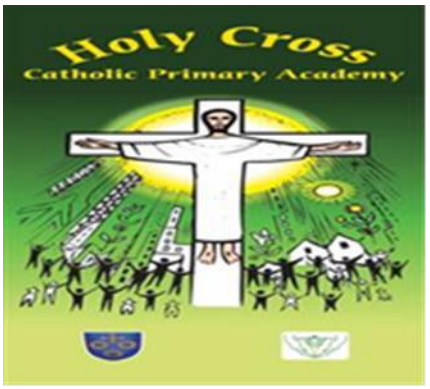


Jesus is the centre of our lives,

Our learning and friendships.

In a safe, happy and caring community

Where all are welcome.

HOLY CROSS CATHOLIC PRIMARY ACADEMY

E-SAFETY POLICY

JANUARY 2025

REVIEW JANUARY 2027

E-Safety (Digital Safety) Policy

Holy Cross Catholic Primary Academy

Mission Statement

This Policy has been written in line with our School's Mission Statement.

Jesus is the centre of our lives,

Our learning and friendships.

In a safe, happy and caring community

Where all are welcome.

Scope of the Policy

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

Headteachers to such an extent as is reasonable, may regulate the behaviour of pupils when they are off the school site and members of staff may be empowered to follow sanctions as per the school's Positive Relationships and Behaviour Policy for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other E-Safety incidents covered by this Policy, which may take place outside of the school, but is linked to membership of the school.

Our 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 E-Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy. The Safeguarding Link Governors will monitor E-Safety within their remit and will report to the GB within their safeguarding report.

Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community. The Headteacher (Designated Safeguarding Lead) and Deputy Safeguarding Lead/s are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Liaises with the external support company.
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.

Technical staff:

The Computing Lead is responsible for ensuring that in liaison with the school computing support company;

- That our school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That our school meets required E-Safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection
- That filtering is applied and updated on a regular basis.
- That they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- To monitor any misuse / attempted misuse that needs to be reported to the Headteacher for investigation

Teaching and Support Staff: are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety Policy and Practices
- They have read, understood and signed the Staff Code of Conduct Policy
- They report any suspected misuse or problem to the Headteacher/Computing Lead for investigation, action or sanction
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems (not via social media)
- E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the E-Safety and acceptable use policies

- Pupils are developing a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Any lessons where internet use is pre-planned, pupils 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: is trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding 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.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy;
- Are developing 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;
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school;
- Continue to develop their understanding of 'digital footprint' and being responsible users

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 parent evenings, newsletters, letters, website and information about national / local E-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-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 learning platforms

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-Safety is therefore an essential part of the school's E-Safety provision. Children need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce E-Safety messages across the curriculum. The E-Safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned E-Safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited
- Key E-Safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to develop their ability to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Pupil 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 pupils 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
- Pupils should be helped to understand what a 'digital footprint is' and how their choices can affect it

Education – parents / carers

Parents may underestimate how often children 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, website

• Parents / Carers evenings / sessions

• High profile events / campaigns e.g. Safer Internet Day

• Reference to the relevant web sites / publications

e.g. www.saferinternet.org.uk/http://www.childnet.com/parents - and - carers

www.thinkyouknow.co.uk (CEOP).

Education & Training – Staff / Volunteers

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

- All new staff as part of their induction programme, will be given the school E-Safety Policy, Staff Code of Conduct and Pupil Acceptable Use Agreements
- The Computing Lead will receive regular updates through attendance at training events and by reviewing guidance documents released by relevant organisations
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings
- The Computing Lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in E-Safety training / awareness sessions

Governors should participate in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons)

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 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 E-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 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

- Headteacher, Computing lead and Finance Assistant are 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. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provider and also by the school's computing support company.

- The school has provided enhanced / differentiated user-level filtering. (Staff/Pupil)

- School technical staff regularly monitor 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 (Headteacher or Senior Leadership), as agreed

- 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 agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems

Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

- The school will maintain a photographic permission register for all pupils and ensure that all staff are aware of any pupil in their class who has not permission to be photographed

- Parents / carers are welcome to take 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 pupils 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs

Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR Act 2016.

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.

Our school must ensure that:

- 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 and a Data Handling Security Policy.

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
- Staff who have to transfer data use encryption and secure password protected devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school Policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications' technologies has the potential to enhance learning. 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. Staff and pupils 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, 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 pupils 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
- Pupils should be taught about E-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 have a duty of care to provide a safe learning environment for pupils and staff.

Schools 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:

- Staff Code of Conduct.
- Information about 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 school staff should ensure that:
    - No reference should be made in social media to pupils, 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
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for	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**	

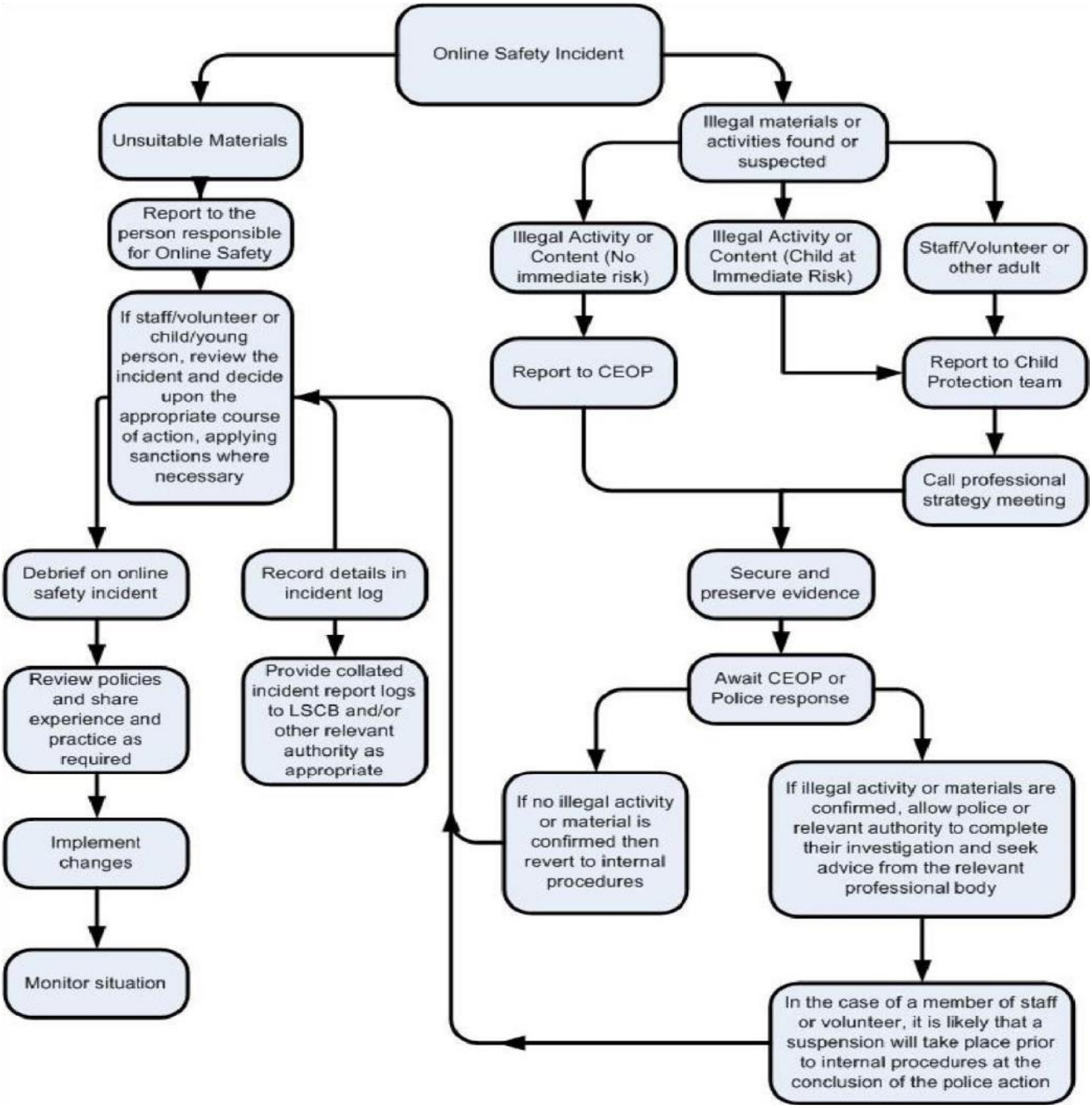
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school			**x**		
Infringing copyright				**x**	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				**x**	
Creating or propagating computer viruses or other harmful files				**x**	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				**x**	
Online gaming (educational)			**x**		
Online gaming (non-educational)			**x**		
Online gambling				**x**	
Online 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.



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:

- 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.

- 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.

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.

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.