Online Safety
POLICY

Document History	
CREATED: (Updated)	Autumn 15
By:	SLT
Version:	1
REVIEW FREQUENCY:	Annually
APPROVED BY GOVERNING BODY:	Summer 2016
REVIEW DATE:	Summer 2018

Online Safety POLICY

The school will monitor the impact of the policy using:

- *Logs of reported incidents.*
- *Questionnaires of pupils, parents and staff.*

Scope of the Policy

This policy applies to all members of the school (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 Inspectors Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary sanctions for inappropriate and unacceptable behaviour. This is pertinent to incidents of cyber-bullying, or other online-safety incidents covered by the 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 and associated behaviour and anti-bulling 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 outlines the e-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. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of ‘Safeguarding’ Governor and Online Safety comes under this. The role of the Online safety Governor will include:

- *Regular meetings with the Online Safety Leader.*
- *Regular monitoring of the Online Safety incident logs.*
- *Reporting to relevant Governors meeting.*

Head Teacher and Senior Leaders:

- The Head Teacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head Teacher and Senior Leaders are responsible for ensuring that the ICT (Online Safety) Leader 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 Teacher 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 currently the Head Teacher. The school is monitored by 'Policy Central.'

Online Safety Leader (Currently the Head Teacher / Mr Coldwell):

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school technical staff.
- Receives reports of online safety incidents and creates a log of incidents to inform online safety developments.
- Meets with the safeguarding governor to discuss current issues, review incident logs.
- Attends relevant governors meetings.
- Reports regularly to the Senior Leadership Team.

Technical Staff (OneIT):

The leader of ICT, School Business Manager and Head Teacher are responsible for ensuring that OneIT ensure:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and the Online Safety Policy.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- 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.

- That the use of the network / internet / virtual learning environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher / Senior Leader / ICT Leader. This is currently done by the Head Teacher.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters including the PREVENT Duty (2015) and of the current academy online safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).
- They report any suspected misuse or problem to the Head Teacher for investigation / action / sanction.
- All digital communications with 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.
- Pupils understand and follow the online safety and acceptable use policies.
- They monitor the 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 the 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 suitable material that is found in internet searches.

Child Protection / Safeguarding Designated Person/s:

Should be trained in online safety issues including PREVENT, 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.
- Radicalisation.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the pupil acceptable use policy.
- 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 policies on the taking / use of images and on cyber-bulling.
- 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 consultation time, newsletters, 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.

Community Users:

Community users who access school systems / website as part of the wider school provision e.g. Education Welfare Limited will be expected to sign a Community User AUA before being provided with access to school systems.

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 online safety is therefore an essential part of the schools online safety provision. Children and young people need the help and support of the school to recognise and avoid 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 / PSHE / other lessons and should be regularly revisited.**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies.**

- **Pupils should be taught in all lessons to be aware of the materials / content they access online and be guided to validate the accuracy of information.**
- 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 the 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such situations, staff can request that the technical staff (through the School Business Manager (SBM)) can temporarily remove these 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 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:

- *Curriculum activities.*
- *Letters, newsletters and website.*
- *Consultation time.*
- *High profile events e.g. National Anti - Bullying Week.*

Education – The Wider Community

The school will provide opportunities for 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 Academy's website will provide online safety information for the wider community.

Education & Training – 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:

- Formal online safety training will be given annually to all staff at the beginning of each academic year or through induction if they start later. Through induction all new staff should fully understand the school e-safety policy and Acceptable Use Agreements.
- The Online safety/ICT Leader will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) and by reviewing guidance documents released by organisations.
- The Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety / IT Leader will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions with particular importance for those who are involved in safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the LA / or other relevant organisation.
- Participation in school training / information sessions for staff.
- Through presentation at the Standards Committee meeting.

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 the 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 academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the academy technical systems.
- Server, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to the academy technical systems and devices.

- The Head Teacher / School Business 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.
- Policy Central and the Head Teacher 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. All staff are to report any actual / potential technical incident to the SBM / Technician and any security breach to the Head Teacher.
- Appropriate security measures are in place to protect 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's infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy 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 cyber – 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of the images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. 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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff 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 for 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.
- Written permission from parents / carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with permission of the pupil and parents / carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- *Fairly and lawfully processed.*
- *Processed for limited purposes.*
- *Adequate, relevant and not excessive.*
- *Accurate.*
- *Kept no longer than necessary.*
- *Processed in accordance with the data subject's rights.*
- *Secure.*
- *Only transferred to others with adequate protection.*

The 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.**
- Responsible persons are identified – School Business Manager / Head Teacher.

- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights to 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 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.**

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & Other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√							√
Taking photos on mobile phones				√				√
Taking photos on school cameras, portable devices including ipods.	√						√	
Use of personal email addresses in school, or on school network		√						√

Use of school email for personal emails		√						√
Use of social media				√				√
Use of blogs (school blog)	√				√			

When using communication technologies the school considers the following good practice:

- **The school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** Staff and pupils should therefore use only the school email service to communicate with others in school, or on school systems.
- **Users must immediately report, to the nominated person –** 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 parents / carers, students and volunteers (email) must be professional in tone and content.** These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- **No digital communication must be made between staff and pupils.**
- Whole class email addresses may be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught e-safety issues, such as the risks attached to 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

(See also the school's Social Networking Policy)

All schools have a duty of care to provide safe learning environments 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, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school 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.

- Training to include: acceptable use; social media risks; checking 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 at follows:

		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 Contrary to the Criminal Justice and Immigration Act 2008.					X
	Criminally racist material in the 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 to 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 academy.					X	
Infringing copyright					X	

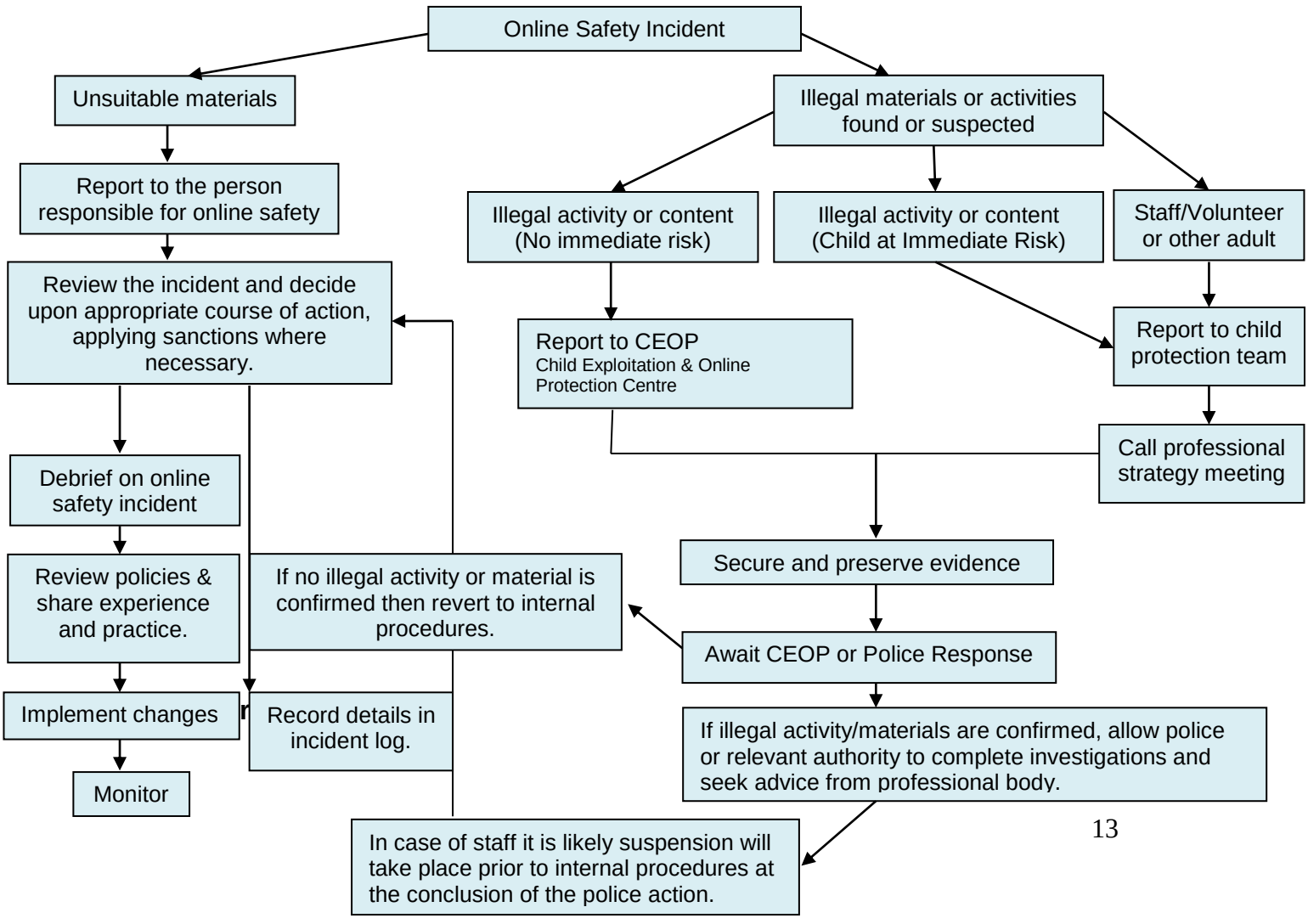
Revealing or publishing confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords).				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line shopping / commerce		X	X		
File sharing			X		
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

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

Illegal Incidents

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



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 the 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 pupils 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 causing concern (these may have already been captured by Policy Central). 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 LA 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.
  - Incidents of radicalisation.
  - 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 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 references purposes.

School Actions and 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 as follows:

Pupils

Incidents	Refer to class teacher	Refer to Head Teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	warning	Further sanctions
Deliberately accessing or trying to access materials that could be considered illegal.		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email	X				X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing usernames and passwords	X						X	
Attempting to access or accessing the school network, using another pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users	X			X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X			X
Continued infringements of the above, following previous warnings and sanctions		X		X		X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X				X
Using proxy sites or other means to subvert the school's filtering system					X		X	
Accidently accessing offensive or pornographic material and failing to report the incident	X	X		X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff

Incidents	Refer to line manager	Refer to Head Teacher	Refer to HR	Refer to technical support staff for action re filtering / security etc	Refer to Police	warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access materials that could be considered illegal.	X	X			X			X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X			X		X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X			X		X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X		X		X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X		X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X		X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	X
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material					X		X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings and sanctions		X					X	X