



## **Telford Infant School**

### **LOVING LEARNING**

**Every child to be an inquisitive, resilient and successful learner who is eager for their next challenge.**

### **Online Safety Policy**

<b>Manager:</b>	Computing Subject Leader
<b>Date of latest update:</b>	March 2023
<b>Date of next review:</b>	March 2024

*This Policy is available for Staff and Governors on the Learning Platform.*

This policy will be reviewed annually in line with the school's policy review programme, or before, if the need arises due to developments. The Computing Subject leader is responsible for reporting to the Governing Board about the quality of its implementation and its impact on standards. In the light of this, policy amendments may be made.

## Introduction

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 ICT systems, both in and out of the school.

It should be read in conjunction with the Information Security Policy, Data Protection Policy, Privacy Notice and Safeguarding Policy.

## 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 Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Safeguarding Governor receiving regular information about Online Safety incidents and monitoring reports. The Safeguarding Governor has taken on the role of Online Safety Governor.

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of Online Safety incident logs
- reporting to relevant the full governing body.

### **Headteacher**

- The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community.
- The Headteacher 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 Online Safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher 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.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

### **Online Safety Co-ordinator**

- 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.
- Provides training and advice for staff
- Liaises with the Local Authority ICT Development Service
- Liaises with school technical staff

- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- Meets at least termly with Online Safety Governor to discuss current issues and review incident logs
- Attends relevant meetings of Governors
- Reports regularly to Senior Leadership Team

### **Warwickshire ICT Development Service**

Warwickshire ICT Development Service is commissioned to provide filtering and monitoring services and is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required Online Safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- 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.
- the use of the network / internet / Learning Platform / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction.
- monitoring software / systems are implemented and updated as agreed in school and LA policies.

### **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 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 Headteacher / Online Safety Coordinator 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 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 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.

### **Designated safeguarding lead**

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
- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

### **Online Safety Group**

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the *Online Safety Group* (or other relevant group) will assist the Online Safety Coordinator with:

- the review and monitoring of the school Online Safety policy
- mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the Online Safety provision
- monitoring improvement actions identified

### **Pupils**

Pupils of the school:

- 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
- 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 and 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 (see Privacy Notice)
- use of social networking sites by children and adults in relation to the school or school matters (see use of social networking policy)
- Mobile, smart watches and tablet devices which must not be brought to school by children
- use of parental mobile and tablet devices when inside the school building

## **Community Users**

- Community Users who access school systems / website / WeLearn365 as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. This includes long term supply teacher and students.

## **Education and training**

### **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 school's Online Safety provision. Children need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

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

- A planned Online Safety curriculum should be provided as part of Computing / PSHE 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 critically aware of the materials / content they access on-line
- 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

### **Education – parents and 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 come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg [www.swgfl.org.uk](http://www.swgfl.org.uk) [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>

### **Education – staff and 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. An audit of the Online Safety training needs of all staff will be carried out regularly.
- 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 (e.g. from LA / 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 / team meetings / INSET days.
- The Online Safety Coordinator 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 members of any sub committee / group involved in 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 or pupil lessons.

## **Technical 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. The school commissions Warwickshire ICT Development Service to provide and maintain safe, secure and reliable infrastructure, filtering and monitoring and to ensure that:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by WCC ICT DS who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Class logins are also available for our children.
- The administrator passwords for the school ICT systems, used by ICT DS must also be available to the Headteacher or Computing Manager and kept in a secure place.
- The Computing Manager along with WCC ICT DS 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
- Internet access is filtered for all users. Requests for filtering changes can be made through the ICT DS Service Desk.

- The school has provided enhanced / differentiated user-level filtering for pupils and staff.
- Technical staff use Policy Central to 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.
- Any actual / potential technical incident / security breaches are logged with ICT DS Service Desk.
- 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.
- Guests (e.g. trainee teachers, supply teachers, visitors) can be given a temporary logon to the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- The school's Information Security Policy outlines the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### Bring Your Own Device

Staff are able to access the internet via the BYOND wireless network. The BYOND network has the same level of filtering as the main school network and activity on BYOND is monitored by Warwickshire ICT DS. Access to BYOND is via the normal WeLearn365 username and password which staff must keep safe and secure and not share with others. Staff are able to bring their own devices such as mobile phones which can only be used in non teaching areas of the school during the school hours of 8.45am and 3.20pm. Staff members wishing to use their own laptops/ipads for working purposes must seek the Head Teachers permission before doing so.

### Digital 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.
- 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 the Information Policy, Data Protection Policy and Privacy notices 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website – consent forms are provided when a child starts school but consent can be withdrawn at any time.

## Data Protection Policy

Data will be processed in line with the Data Protection Policy – please refer to this policy separately.

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The table below shows how the school currently allows their use.

Communication Technologies	Staff & other adults			Pupils		
	Not allowed	Allowed at certain times	Allowed	Not allowed	Allowed at certain times	Allowed
Personal mobile phones for non photo use		X		X		
Personal smart watches for non photo use		X		X		
Personal mobile phones for taking photos	X			X		
Personal smart watches for taking photos	X			X		
Personal tablets for non photo use			X	X		
Personal tablets for taking photos	X			X		
School iPads			X			X
Use of personal email address in school		X		X		
Use of school email address for personal use	X			X		

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 pupils should therefore use only the school email service to communicate with others when 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 pupils or parents / carers (email, chat, WeLearn365 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.
- Whole class / group email addresses may be used at KS1
- Pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

### **Online Activity Restrictions**

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

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 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 or local authority
- 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 nominated	Unacceptable	Unacceptable and illegal
<b>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:</b>	<b>Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978</b>					X
	<b>Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.</b>					X
	<b>Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008</b>					X
	<b>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</b>					X
	<b>pornography</b>				X	
	<b>promotion of any kind of discrimination</b>				X	
	<b>threatening behaviour, including promotion of physical violence or mental harm</b>				X	
	<b>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</b>				X	
<b>Using school systems to run a private business</b>					X	
<b>Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy</b>					X	
<b>Infringing copyright</b>					X	
<b>Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)</b>					X	
<b>Creating or propagating computer viruses or other harmful files</b>					X	
<b>Unfair usage (downloading / uploading large files that hinders others in their use of the internet)</b>					X	
<b>On-line gaming (educational)</b>			X			
<b>On-line gaming (non educational)</b>					X	
<b>On-line gambling</b>					X	
<b>On-line shopping / commerce</b>				X		
<b>File sharing</b>		X				
<b>Use of social media</b>			X			

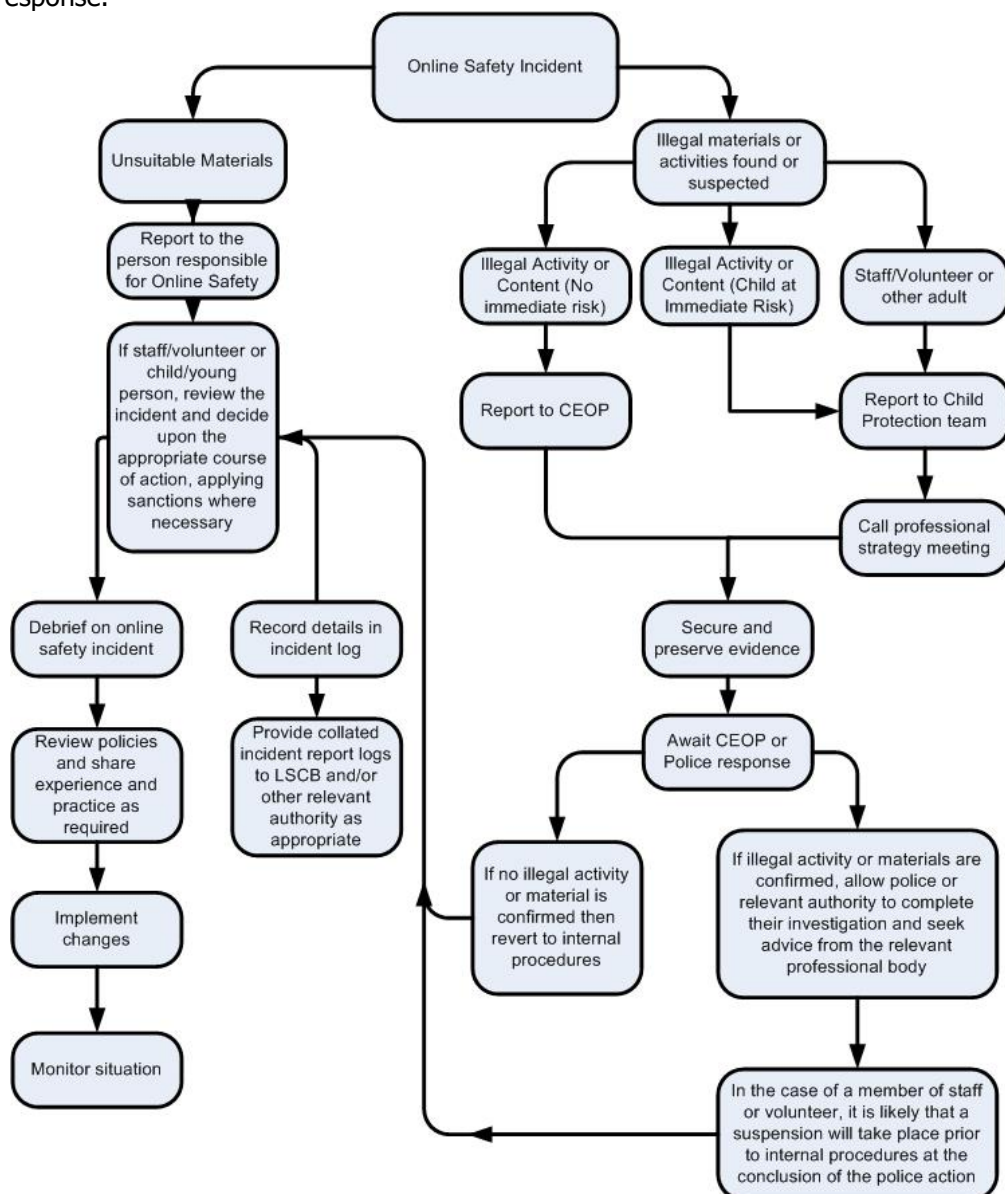
Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

## 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).

**Warwickshire ICT DS will contact the Headteacher if any incident of misuse is detected. If the incident is illegal then the police will be contacted immediately.**

If inappropriate incidents are noticed by school staff then the flowchart below can be used to identify the correct response.



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.

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.

## **Misuse – Actions and Sanctions**

It is more likely that the school / academy 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

## Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	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 sanction eg detention / exclusion
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X					
Unauthorised use of non-educational sites during lessons			X						
Unauthorised use of mobile phone / digital camera / other mobile device			X						
Unauthorised use of social media / messaging apps / personal email			X						
Unauthorised downloading or uploading of files			X						
Allowing others to access school / academy network by sharing username and passwords	X	X	X						
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X	X						
Attempting to access or accessing the school / academy network, using the account of a member of staff			X						
Corrupting or destroying the data of other users			X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X						
Continued infringements of the above, following previous warnings or sanctions			X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						
Using proxy sites or other means to subvert the school's / academy's filtering system			X						
Accidentally accessing offensive or pornographic material and failing to report the incident			X						
Deliberately accessing or trying to access offensive or			X						

pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X						

## Staff

## Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X						
Unauthorised downloading or uploading of files		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						
Careless use of personal data eg holding or transferring data in an insecure manner		X						
Deliberate actions to breach data protection or network security rules		X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X						
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X						
Using proxy sites or other means to subvert the school's / academy's filtering system		X						
Accidentally accessing offensive or pornographic material and failing to report the incident		X						

Deliberately accessing or trying to access offensive or pornographic material		X						
Breaching copyright or licensing regulations		X						
Continued infringements of the above, following previous warnings or sanctions		X						