Sound & District Primary School

Our Children are the Future

Policy written by:	Hannah Poppleton (ICT & E-Safety Coordinator)
Governor Committee:	Achievements and Standards
Date approved by Governing body:	June 18
Review date:	June 2020

E-SAFETY POLICY

Development of this Policy

This E-Safety policy has been developed by a number of stakeholders:

Laura Minshall Thomas	Head teacher
Hannah Poppleton	ICT & E-Safety Coordinator
	Teachers, Support Staff and Non-Teaching staff
Dr Anthony Shuker	ICT Governor
	Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This E-safety policy was approved by the Governing Body on:	
The implementation of this E-safety policy will be monitored by the:	ICT & E-Safety Coordinator
Monitoring will take place at regular intervals:	Every term
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	October 2018
Should serious E-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Reported incidents by adults working within the school.
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of:
  - pupils
  - parents / carers
  - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers 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 penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, 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. 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 schools Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and 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. This will be carried out by the ICT link Governor, receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of ICT Governor. The role of the ICT Governor will include:

- meetings with the ICT & E-Safety Co-ordinator
- give regular updates from the ICT & E-Safety Co-ordinator on any incidents
- monitoring of filtering
- reporting to the Governing Board.

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT & E-Safety Co-ordinator.
- 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. (See flowchart "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Head teacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-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 e-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 liaise with the ICT & E-Safety Coordinator to discuss any incidents.

ICT & E-Safety Coordinator:

- Takes day to day responsibility for e-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 the Local Authority where necessary.
- Liaises with school ICT support.

- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- In contact with/reports to the ICT Governor to discuss current issues and review practice.
- Remains 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.

School's ICT Support

The School's ICT Support is responsible for ensuring:

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

Local Authority Support

The Local Authority is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the required e-safety technical requirements and any Local Authority Guidance that may apply.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That the use of the network, internet and email is regularly monitored in order that any misuse or attempted misuse can be reported to the ICT & E-Safety Coordinator for investigation.
- That monitoring software and systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

All 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 this document
- They report any suspected misuse or problem to the ICT & E-Safety Co-ordinator and if not available, the Head Teacher.
- All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the age related e-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.

Safeguarding Officer(s)

The Safeguarding Officer(s) should be trained in e-safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal or inappropriate materials
- Inappropriate on-line contact with strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils:

All pupils should be:

- Responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy, relevant to their age.
- 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 and use of images and on cyber-bullying.
- 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

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and 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 and local e-safety campaigns and 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 school blogs.
- Their children's personal devices in the school (where this is allowed)

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 and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum should be provided as part of Computing, PHSE and other lessons and should be regularly revisited
- Key e-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 content they access on-line and be guided 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 pupils 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 e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children’s on-line behaviours. Parents and carers 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, website.
- Parents and Carers open evenings with Cheshire East Police & NEP.
- High profile events, e.g. Safer Internet Day.
- Reference to the relevant web sites

Education & Training – All Staff and 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:

- A planned programme of formal e-safety training will be made available to staff. This will be updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use agreements).
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings or INSET days.
- The E-Safety Coordinator will provide guidance and training to individuals/volunteers as required.

Training – Governors

Governors should be encouraged to take part in e-safety training sessions, with particular importance for those who are members of any subcommittee involved in health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority.
- Participation in school training and information sessions for staff or parents.
- Identified 3rd party.

Technical – Infrastructure /equipment, filtering and monitoring

It is important that the managed service provider is fully aware of the school E-Safety Policy and the acceptable use agreements.

The school will be responsible for ensuring that the school 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 school technical systems.
- All users will have clearly defined access rights to school technical systems and devices.
- The “administrator” passwords for the school ICT system, used by the ICT & E-Safety Co-ordinator must also be available to the Head teacher or other nominated senior leader and kept in a secure place.
- Internet access is filtered for all users ensuring only safe content is accessed. Content lists are regularly updated and internet use is logged and regularly monitored.
- An appropriate system is in place for users to report any actual or potential technical incidents to the relevant person, 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. The school infrastructure and individual workstations are protected by up to date anti-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.

- Temporary access to the school systems is available for guests, visitors and supply teachers.
- An agreed policy is in place regarding the extent of personal use that users such as staff, pupils and community users and their family members are allowed on school devices that may be used out of school.

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 and 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 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 and carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be made publicly available on social networking sites, nor should parents and carers comment on any activities involving other pupils in the digital or video images.
- Staff and volunteers are allowed to take digital 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 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
- Pupil's work can only be published with the permission of the pupils and parents and carers.

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.

Communication Technologies	Staff & other Adults				Pupils			
	Allowed	wed at certain times	ed for selected staff	Not allowed	Allowed	wed at certain times	ith staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on personal mobile phones / cameras				X				X
Taking photos using school technology.	X					X		
Use of other mobile devices eg tablets, gaming devices		X					X	
Use of personal email addresses in school, or on school network	X						X	
Use of school email for personal emails	X							X
Use of messaging apps		X						X
Use of social media		X						X
Use of school blogs	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 (e.g. by remote access).
- Users must immediately report to any member of staff 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, pupils or parents and carers (through email, 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- (See Social Media Policy)

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Teachers professional conduct expectations are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

The school provides the following measures to ensure reasonable steps are in place to reduce 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.

All School staff should ensure that:

- No reference should be made in social media to pupils, parents and 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 reduce risk of loss of personal information.

Unsuitable Activities

Some internet activity, e.g. accessing child abuse images or distributing racist material, is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in 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 school staff	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 / academy					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	

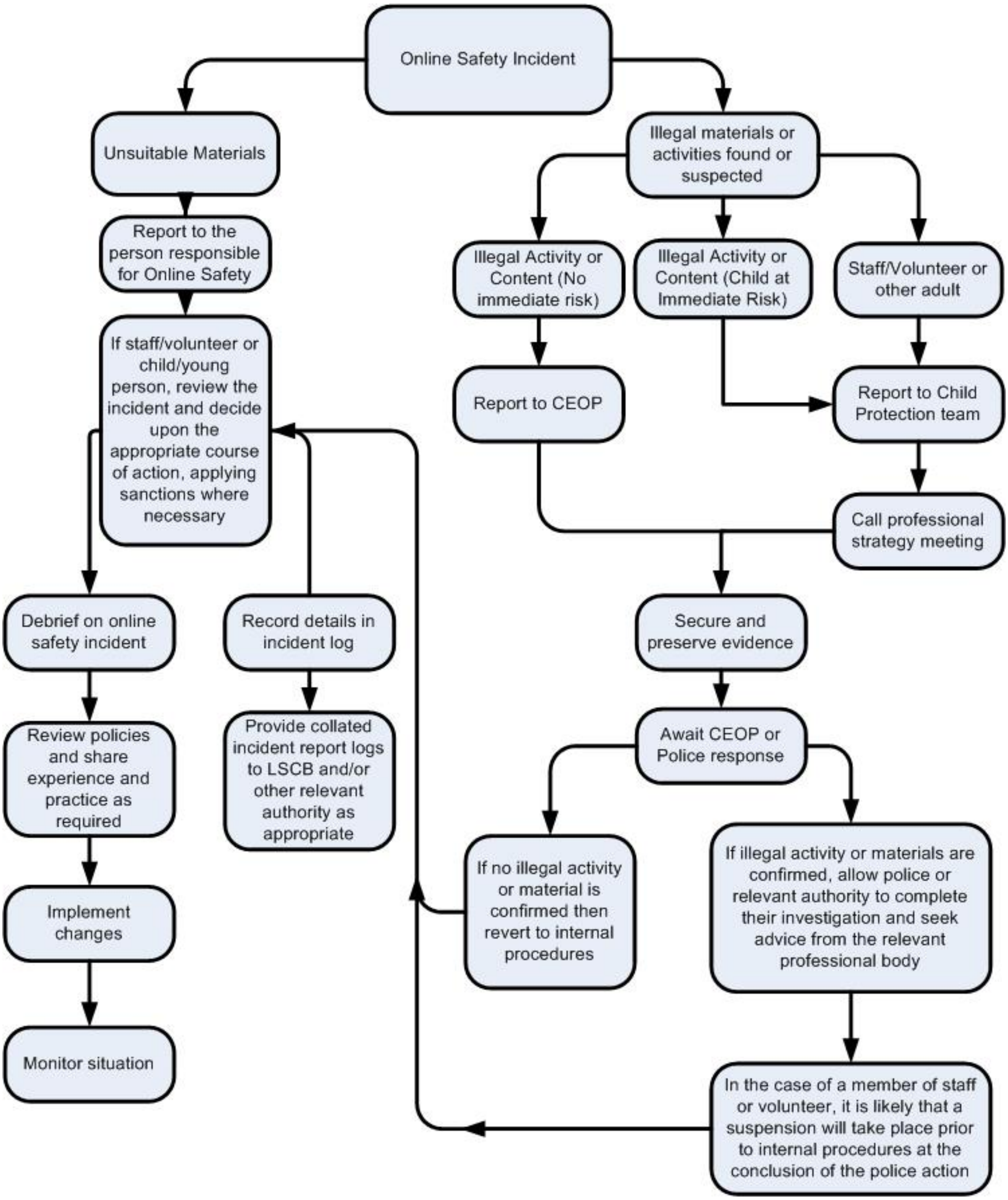
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

Responding to incidents of misuse

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

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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy 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 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. Ensure you 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
  - 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.

Ensure you Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Statutory Duties
The duty to prevent children and young people being radicalised is set out in the following documents.

- Counter Terrorism and Security Act (2015)
- Keeping Children Safe in Education (2015)
- Prevent Duty Guidance (2015)
- Working Together to Safeguard Children (2015)

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy 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. (See Appendix 1).

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 disciplinary procedures as follows:

Pupils **Actions**

Incidents:	Refer to class teacher	Refer to Head or Deputy Head	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Further sanction / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		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			X		
Unauthorised downloading or uploading of files		X			X		
Allowing others to access school network by		X			X		

sharing username and passwords							
Attempting to access or accessing the school network, using another pupil’s account	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	X					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X		
Continued infringements of the above, following previous warnings or sanctions		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			X		
Deliberately accessing or trying to access offensive or pornographic material	X	X			X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X		

Staff **Actions**

Incidents:	Refer to Head teacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on inappropriate activities).	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			
Careless use of personal data e.g. 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 pupils	X	X		

Actions which could compromise the staff member's professional standing	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 filtering system	X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	
Breaching copyright or licensing regulations	X			
Continued infringements of the above, following previous warnings or sanctions	X			

Foundation Stage and Key Stage 1
Pupil Acceptable Use Agreement

I want to feel safe all of the time!

- I will only do things on a computer or iPad which my teacher says is OK.
- I will only work with people I know in real life.
- I will tell my teacher if anything makes me feel scared or uncomfortable or I do not understand.
- Make sure all messages I send are polite and kind.
- I will not reply to any nasty message or anything which makes me feel uncomfortable.
- I will talk to my teacher before using anything on the internet.
- I will not play games (unless told to by my teacher) during lesson time.
- I will not tell people about myself online (I will not tell them my name, anything about my family and home, phone numbers or pets).
- I will not load photos of myself onto the computer.
- Never agree to meet a stranger.

I have read and understand these rules and agree to them.

Signed: Date:

Foundation Stage and Key Stage 1
Parent Acceptable Use Agreement

As the parent and carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed: Date:
Child's name:
Relationship to the child

Key Stage 2
Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers and iPads for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep any logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a member of staff.

I have read and understand these rules and agree to them.

Signed: Date:

Key Stage 2
Parent Acceptable Use Agreement

As the parent andcarer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed: Date:

Child's name:

Relationship to the child:

Staff (and Volunteer) Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT where necessary to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will only communicate with pupils and parents and carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless agreed by the ICT & E-safety coordinator.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy. Protected and Restricted data must be held in encrypted storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, in the ICT log book and contact the ICT co-ordinator.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- That community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- That school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user’s files, without permission.
- I will ensure that if I take any/or publish images of others I will only do so with permission from the school. I will not use my personal equipment to record these images, without permission.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school devices.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed □ Date □

Appendix 1
Responding to incidents of misuse – flow chart

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Appendix 2
Template Reporting Log

Reporting Log Group						
Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 3
Training Needs Audit

Training Needs Audit Log Group .... Date						
Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
ICT	Information and Communications Technology
LA	Local Authority
OFSED	The Office for Standards in Education, Children's Services and Skills.