MANOR ROAD PRIMARY SCHOOL

ONLINE SAFETY POLICY

September 2026

Manor Road Primary School
Online Safety Policy

Contents

Page	Details
3	Policy Development and Review
3	Scope of the Policy
4	Roles and Responsibilities
7	Policy Statements
7	Education : Parents and the Wider Community
8	Training : Staff, Volunteers and Students
9	Training : Governors
9	Technical Infrastructure / Equipment, Filtering and Monitoring
10	Mobile Technologies
10	Use of Digital and Video Images
11	PREVENT
12	Data Protection
13	Communications
14	Social Media
16	Responding to Incidents of Misuse
23	Review Schedule

Manor Road Primary School
Online Safety Policy

DEVELOPMENT AND REVIEW

This Online Safety Policy has been developed by:

- Headteacher and Deputy Headteacher
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users

Schedule for Development/Monitoring/Review

- The implementation of this policy will be monitored by the Headteacher/SMT
- Monitoring will take place annually
- The Governing Body will receive a report, generated by the Online Safety Group, on the implementation of the policy at regular intervals where appropriate
- The Online 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 online safety or incidents that have taken place
- Should serious on-line safety incidents take place the LA, Police, Children's Social Care maybe be informed

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents/ carers and staff

SCOPE OF THE POLICY

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

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

ROLES AND RESPONSIBILITIES

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 online safety incidents and monitoring reports.

The Chair of Governors, is responsible for Safeguarding and Child Protection.

The Online Safety Governor is Adam Hayhurst.

The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Leader
- Attendance at Online Safety Group meetings
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors meetings

Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Leader.
- 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. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures)
- The Headteacher and Senior Leaders are responsible for ensuring that the 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 Headteacher and Senior Leaders 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 Management Team will receive regular monitoring reports from the Leader

Online Safety Leader:

At Manor Road, the Online Safety Leader is Karen Marshall

- Leads the Online Safety Group
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant Governors meetings
- Reports regularly to Senior Leadership Team

Computing Subject Leader:

At Manor Road, the Computing Subject Leader is Brogan Lawrenson

The Computing Subject Leader 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 required online safety technical requirements and any Local Authority Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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 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
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Senior Leader for investigation/action/sanction
- That monitoring software/systems are implemented and updated as agreed in school 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 or Senior Leader
- 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 Policy and Acceptable Use Policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons, where internet use is pre-planned, 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:
  a) sharing of personal data
  b) access to illegal / inappropriate materials
  c) inappropriate on-line contact with adults / strangers
  d) potential or actual incidents of grooming

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. This group may be part of a safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Leader with:

- The production/review/monitoring of the school's Online Safety Policy/documents.
- The production/review/monitoring of the school filtering system and requests for filtering changes.
- 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 pupils about the online safety provision
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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-bullying.
- 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:

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 on-line safety campaigns/literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website and on-line pupil records
- Their children's personal devices in the school (when this is allowed)

Community Users:

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA

POLICY STATEMENTS

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

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited (see Kapow scheme of work)
- Key online safety messages should be reinforced as part of a planned programme of assemblies/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy 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:

Some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's online 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

- Letters, newsletters, website
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

The Wider Community:

The school will provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- 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 school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/ sports/ voluntary groups to enhance their online safety provision

TRAINING

Staff, Volunteers and Students:

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's Online Safety Policy and Acceptable Use Policy.

- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Leader (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL/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/meetings and INSET days.
- The Online Safety Leader (or other nominated person) will provide advice/ guidance /training to individuals as required.

Governors:

Governors may take part in online safety training/awareness sessions, with particular importance for those who are involved in technology/on-line safety/health and safety/ safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents

TECHNICAL INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING

The school will ensure that appropriate filtering, monitoring and technical security measures are in place to safeguard pupils, staff and school systems.

- The school uses **Netsweeper** and **PTeS** to provide filtering and monitoring of online activity.
- Internet access is filtered to protect users from inappropriate, harmful, extremist and illegal content, including content identified through the Internet Watch Foundation (IWF) list.
- Internet activity is logged and monitored, and filtering settings are reviewed regularly to ensure they remain effective and age-appropriate.
- Monitoring alerts are reviewed promptly by authorised staff, including the Designated Safeguarding Lead (DSL) and Deputy DSLs.
- Any safeguarding concerns identified through monitoring systems will be managed in accordance with the school's Safeguarding and Child Protection Policy.
- The school will maintain secure networks, devices and infrastructure through the use of appropriate security measures, including firewalls, antivirus software and access controls.
- Servers, wireless systems and network equipment will be securely located, with physical access restricted to authorised personnel.
- All users will be assigned individual usernames and secure passwords and will be responsible for maintaining their confidentiality.
- Access to school systems will be allocated according to users' roles and responsibilities.
- Regular reviews and audits of the school's filtering, monitoring and technical security arrangements will be undertaken.
- Software licences will be monitored to ensure compliance with licensing agreements.

- Procedures will be in place to manage guest access, software installation, use of removable media and the use of school devices outside school.
- Any actual or suspected security breach must be reported immediately to the Headteacher or a member of the Senior Leadership Team.
- Personal data will only be transferred or stored outside the school's secure systems where appropriate security measures, including encryption, are in place.
- Governors and senior leaders will regularly review the effectiveness of filtering, monitoring and technical security arrangements as part of the school's safeguarding responsibilities.

MOBILE TECHNOLOGIES

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding & Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The School Acceptable Use Agreements for staff, volunteers, students, pupils and parents/carers will give consideration to the use of mobile technologies.

The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in School	Yes	Yes	Yes	Yes	Yes	Yes
Full Network Access	Yes	Yes	Yes	No	No	No
Internet Only				No	Yes	Yes

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide

avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. 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. See Appendix 12 for the Pan-Lancashire LSCB Online Safeguarding Group 'Sexting in Schools & Colleges: Flowchart for responding to incidents'.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- 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 and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

PREVENT

Staff at Manor Road Primary School understand their Prevent duty requirements as part of their wider safeguarding responsibilities as outlined in Keeping Children Safe in Education (KCSIE).

"All schools and registered childcare providers are required to "have due regard to the need to prevent people from being drawn into terrorism".

The school recognises that we should help students build resilience against extremism and radicalisation by fostering a strong ethos and values-based education, as well as by providing a safe space for them to debate controversial issues and develop the critical thinking skills and knowledge they need to be able to challenge extremist arguments.

All teaching staff are able to:

- recognise the signs of someone being radicalised into terrorism
- share concerns in the correct manner
- understand the support available to that person.

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 is 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
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of 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 are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / 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

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

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

COMMUNICATIONS

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

	Staff and Other Adults					Pupils			
	Allowed	Allowed at certain times with permission of SLT	Allowed for selected staff	Not allowed		Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought into school	✓							✓	
Use of mobile phones in lessons				✓					✓
Use of mobile phones in social time	✓								✓
Taking photos on mobile phones / personal cameras				✓					✓
Use of other mobile devices, eg tablets, gaming devices	✓							✓	
Use of personal email addresses in school, or on school network		✓							✓
Use of school email for personal emails			✓						✓
Use of messaging apps for school related activities	✓								✓
Use of social media			✓						✓
Use of blogs			✓					✓	

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 / ac systems (e.g. by remote access)
- 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, social media, chat, blogs, VLE 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, while pupils at KS2 and above will be provided with individual school email addresses for educational use
- 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

SOCIAL MEDIA

Protecting Professional Identity

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:

- Ensuring that personal information is not published
- Training is provided including: 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

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
  i) Systems for reporting and dealing with abuse and misuse
  ii) Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

The school's use of social media for professional purposes will be checked regularly by the Headteacher and Online Safety Group to ensure compliance with the school policies.

Unsuitable/Inappropriate 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 / or outside the school when using school equipment or systems.

The school restricts usage as follows:

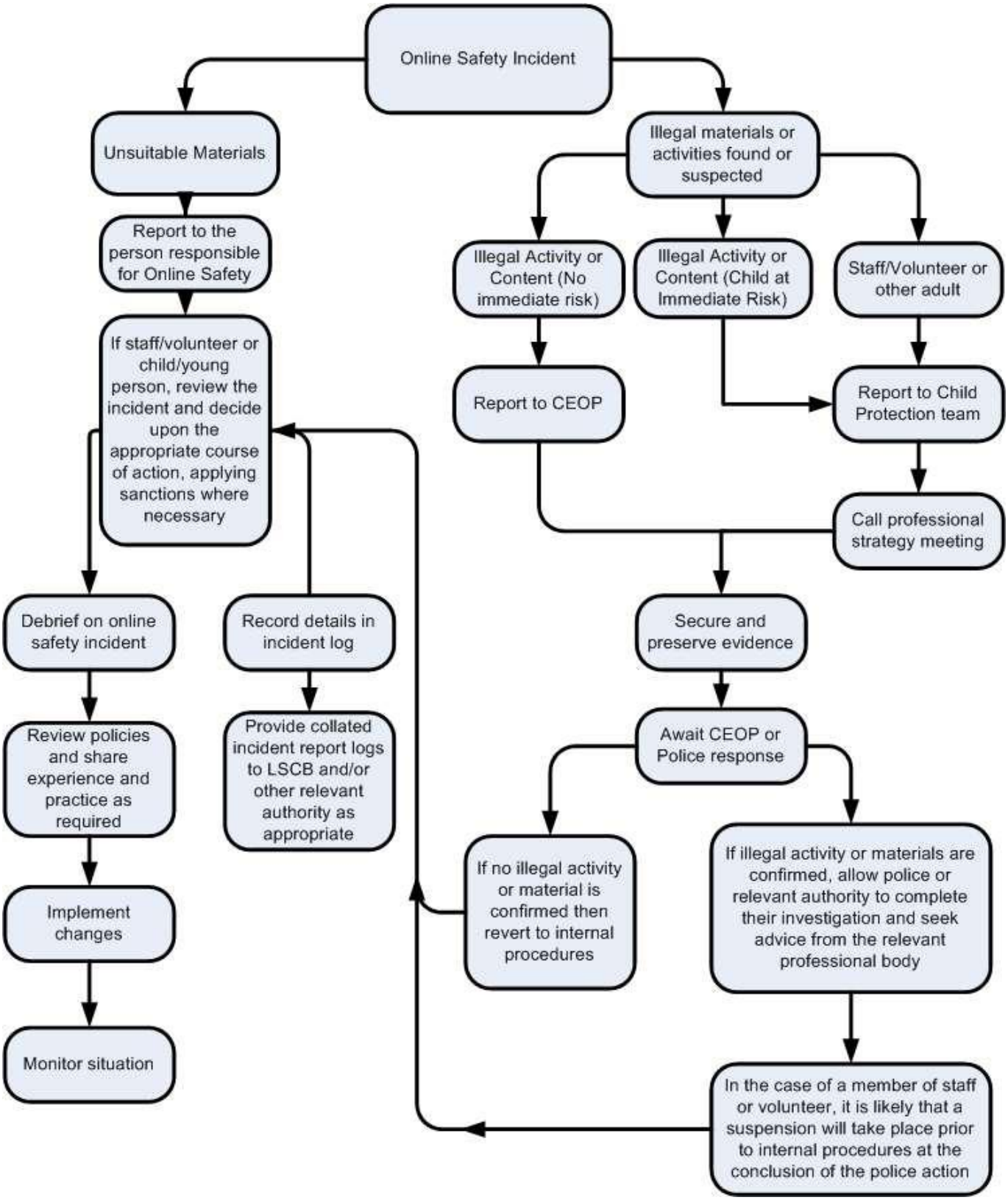
USER ACTIONS		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unaceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – the making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008					✓
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	Threatening behaviour, including promotion of physical violence or mental harm				✓	
	Any other information which may be offensive to colleagues or breaches the				✓	

	integrity of the ethos of the school or brings the school into disrepute					
Using school to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gaming (non-educational)					✓	
On-line gambling					✓	
On-line shopping / commerce			✓			
File sharing		✓				
Use of social media				✓		
Use of messaging apps			✓			
Use of video broadcasting eg Youtube			✓			

RESPONDING TO INCIDENTS OF MISUSE

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely,

through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following: i) Internal response or discipline procedures
  ii) 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’ behavior
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Staff should isolate the computer in question as best they 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

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	ACTIONS / SANCTIONS								
INCIDENTS	Refer to class teacher	Refer to SLT	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓			✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓			✓	
Unauthorised use of mobile phone / digital camera / other mobile device	✓	✓	✓			✓		✓	
Unauthorised use of social media / messaging apps / personal email	✓	✓	✓			✓		✓	
Unauthorised downloading or uploading of files	✓	✓	✓			✓		✓	
Allowing others to access school / academy network by sharing username and passwords	✓	✓			✓			✓	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	✓	✓	✓		✓	✓		✓	
Attempting to access or accessing the school / academy network, using the account of a member of staff		✓	✓		✓	✓		✓	✓
Corrupting or destroying the data of other users		✓	✓			✓		✓	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓			✓		✓	
Continued infringements of the above, following previous warnings or sanctions			✓		✓	✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓			✓	✓		✓
Using proxy sites or other means to subvert the school's / academy's filtering system			✓		✓		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓			✓		✓	
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓			✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓						✓	

STAFF	ACTIONS / SANCTIONS							
INCIDENTS	Refer to Line Manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to technical support staff for action re	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓			✓
Inappropriate personal use of the internet / social media / personal email		✓	✓			✓		✓
Unauthorised downloading or uploading of files		✓				✓		
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		✓			✓	✓		✓
Careless use of personal data eg holding or transferring data in an insecure manner		✓				✓		✓
Deliberate actions to breach data protection or network security rules		✓	✓		✓	✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓		✓			✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓					✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓	✓					✓
Actions which could compromise the staff member's professional standing		✓	✓			✓		✓
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		✓	✓			✓		✓
Using proxy sites or other means to subvert the school's / academy's filtering system		✓	✓			✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓				✓		✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓					✓
Breaching copyright or licensing regulations		✓				✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓		✓

LSCB 25/17

Pan-Lancashire LSCB Online Safeguarding Group

Sexting in Schools & Colleges: Flowchart for responding to incidents

The flowchart process below is directly taken from the *Sexting in schools & colleges: Responding to incidents and safeguarding young people* guidance produced on behalf of the Government by the UK Council for Child Internet Safety (UKCCIS). It highlights the jointly-recommended process advocated by Lancashire and Blackburn with Darwen Safeguarding Boards in partnership with Lancashire Constabulary for managing and responding to Sexting incidents and includes additional annotations to signpost useful supporting resources and a number of Frequently Asked Questions.

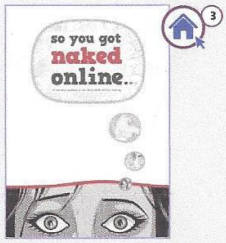
Supporting Resources

Highly Recommended

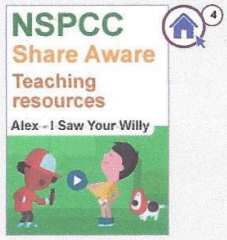
Nationally-recognised best-practice guidance for Schools & Colleges. It is strongly recommended that **all Designated Safeguarding Leads (DSLs) should be expressly familiar with this guidance**

Online Safety Helpline: Highly-recommended helpline for professionals working with Children & Young People seeking further advice and support with online issues

Support For Young People: Practical post-incident advice from SWGfL to support Young People

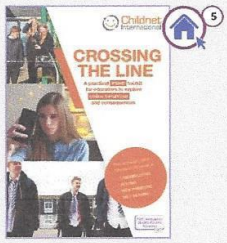


Curriculum delivery: Excellent Key Stage 2 NSPCC Teaching Resources including videos '*I Saw your Willy*' and '*Lucy and the boy*'



Highly Recommended

Curriculum delivery: Very useful PSHE curriculum resource for 11-14 y/o covering a variety of Online Safety areas including Sexting



UKCCIS Flowchart for responding to Sexting incidents

Initial disclosure: This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team: At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about **whether the incident can be dealt with in house**. (For more information see page 13 of UKCCIS Sexting in schools and colleges)

UKCCIS guidance

5 points for referral:
1. **Adult involvement**
2. **Coercion or blackmail**
3. **Extreme or violent**
4. **Under 13**
5. **Immediate risk of harm**

(For more information refer to section 2 of UKCCIS Sexting in schools and colleges)

LSCB Supporting note: If the incident meets the criteria for Police referral, reporting should focus on **describing** rather than **diagnosing** the incident

Police / Social Care / MASH referral
Refer to your local arrangements for dealing with incidents and contact local services. (For more information refer to page 17 of UKCCIS Sexting in schools and colleges)

Risk assessment / Dealing with the incident: Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care. (For more information refer to page 14 and Annex A of UKCCIS Sexting in schools and colleges)

UKCCIS guidance

Considerations – Risk Assessment
-Vulnerability of the child
-Coercion
-How shared and where
-Impact on children
-Age of the children
(For more information see UKCCIS Sexting in schools and colleges - Annex A)

Management in school: Ensure parents are informed and the incident recorded **following all child protection and safeguarding procedures**. (For more information see page 14 of UKCCIS Sexting in schools and colleges)

LSCB Supporting note: Incident review arrangements may include reviewing curriculum provision

Lancashire Safeguarding Boards | Blackburn with Darwen | Lancashire Constabulary – police and communities together

Supporting Resources (Links):

1. UKCCIS Sexting in schools and colleges:
   www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.pdf
2. UKSIC Professionals Online Safety Helpline (POSH):
   www.saferinternet.org.uk/professionals-online-safety-helpline
3. SWGfL – So You Got Naked Online:
   http://childnetsic.s3.amazonaws.com/ufiles/Files%202015/SYGNO%20Booklet%20-%20version%202%20May%202015.pdf
4. NSPCC Share Aware - Key Stage 2 Teacher Resource (Alex)
   www.nspcc.org.uk/globalassets/documents/advice-and-info/lesson_plan_alex.pdf
5. Childnet Crossing the Line PSHE Resource (11-14 y/o):
   www.childnet.com/resources/pshetoolkit

Frequently Asked Questions:

Q: Do I need to report all Sexting instances to the Police and/or Children's Social Care?

No, the Initial Review Meeting should consider whether immediate referral is required according to the 5 criteria outlined on Page 11 of the UKCCIS guidance. If none of these criteria apply, schools may therefore decide it is appropriate to manage the incident locally. However, should further information/concern come to light, then the school can subsequently choose to escalate the incident at any time.

Q: As the DSL, am I allowed to view the image in order to make a decision?

The section 'Searching devices, viewing and deleting imagery' on Pages 15 & 16 of the UKCCIS guidance provides clear examples of circumstances when it may be necessary to view imagery and what actions the DSL should/should not take.

Q: Should I involve parents/carers when dealing with Sexting instances?

The section 'Handling Incidents – Initial response' on Page 10 of the UKCCIS guidance highlights that "*Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm*". Further detailed advice and information regarding involving parents and carers is contained within a dedicated Annex (Annex C) of the guidance on Pages 31-34 and includes guidance around supporting victims and steps that can be taken to get images removed (see also – 'So You Got Naked Online' resource above).

Q: Will the young person get a criminal record if I refer the incident to the Police?

This will depend upon the circumstances and all Sexting incidents reported to the Police will require recording and an investigation (although this is not the same as having a criminal record). Where appropriate, the Police may decide it is not in the public interest to pursue an investigation and further detailed information about this aspect and the Police response can be found on Pages 8 & 9 of the UKCCIS guidance.

Further information about keeping children safe online is available from the LSCB Online Safeguarding website below:

Pan-Lancashire LSCB Online Safeguarding website
www.lancashiresafeguarding.org.uk/online-safeguarding.aspx

Lancashire Safeguarding Boards | Blackburn with Darwen | Lancashire Constabulary – police and communities together

POLICY REVIEW DETAILS		
Policy written by	Brogan Lawrenson	This policy is based on policy and advice documents published by the South West Grid For Learning Trust
Policy implemented	February 2017	Adopted by Governors
Policy reviewed	September 2017	Updated as required
	September 2018	Updated as required
	September 2019	Updated as required
	September 2020	Updated as required
	September 2021	Updated as required Moved onto updated Manor Road format.
	September 2022	Updated as required
	September 2023	Updated as required
	September 2024	Updated as required. Prevent now included
	September 2025	Updated as required. New Online Safety Governor to be appointed at next Full Governor meeting. Amended in November 2025 to include name of new Online Safety Governor.
	September 2026	Updated to include new information about Filtering and Monitoring.
Review schedule	September 2026	