Online Safety Policy

Date this policy was reviewed and by whom	September 2025 by Mr A. Wignall
Date of next review and by whom	September 2026 by Mr A. Wignall

Our School Vision

At Monksdown Primary School we aim high. We want every part of our school community- pupils, parents and members of staff to experience success. Monksdown Primary School will work with everyone to create a happy, safe and stimulating setting where children are motivated to learn together. By maintaining high expectations of ourselves and each other, our children will be equipped to encounter opportunities and challenges with resilience and determination. We encourage a curiosity about the world and strive to ensure that our children will contribute positively, now and in the future.

Headtecher and Designated Safeguarding Lead	Mrs J. Price
Designated Safeguarding Lead (DSL) team	Mrs C. Russell (DSL) Mrs G. Stewart
Online-safety coordinator (if different)	Mr A. Wignall
Online-safety / safeguarding link governor	Mr M. Reynolds
Network manager / other technical support	MGL

Aims

This policy aims to:

- Set out expectations for all Monksdown Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

What is this policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE) and other statutory documents; it is designed to sit alongside Monksdown Primary School's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

This policy also reflects the Department for Education's 2023 guidance on Filtering and Monitoring Standards, and the statutory requirement that DSLs take lead responsibility for online safety, including oversight of filtering and monitoring arrangements.

This policy applies to all members of the school community (staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of the school ICT systems, both in and out of 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 online-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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 inside and outside of school.

Roles and Responsibilities

Headteacher – Mrs J. Price

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Liverpool Safeguarding Children Partnership (LSCP) guidance
- Ensure the DSL and deputies receive specific training on filtering and monitoring systems, and that technical staff and governors receive appropriate briefings
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school’s provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate IT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles

- Ensure that the school has carried out Data Protection Impact Assessments (DPIAs) for monitoring systems and key cloud providers where required, and that third-party suppliers are subject to appropriate due diligence
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles. This includes induction training for all new staff and regular updates (at least annually), with online safety embedded within safeguarding CPD.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Provide governors with an annual report on the effectiveness of the school's filtering and monitoring, including reference to the DfE Standards
- Ensure the school website meets statutory DfE requirements

Designated Safeguarding Leads / Online Safety Co-ordinator –

Certain online-safety duties delegated to Online Safety Co-Ordinator, but not the overall responsibility.

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." [KCSIE 2025]
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate." [KCSIE 2025 and DfE guidance]
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the head teacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

- Stay up to date with the latest trends in online safety
- Ensure the DSL/OSL understands the school’s filtering and monitoring solution (Smoothwall) — how to access logs, run reports, acknowledge alerts and maintain a change-control log of any filter adjustments
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees
- This policy and the school’s filtering & monitoring provision will be reviewed at least annually and after any significant change to technology, any safeguarding incident involving online content, or when new national guidance is published
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- This policy and the school’s filtering & monitoring provision will be reviewed at least annually and after any significant change to technology, any safeguarding incident involving online content, or when new national guidance is published
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- All online-safety incidents will be logged on CPOMS (or equivalent) and linked to other safeguarding records where appropriate; details of monitoring alerts and actions taken should be stored securely and retained in line with DPO advice
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors (is it physical or technical?) and ensure staff are aware
- Ensure the monitoring approach balances technical monitoring with physical supervision and education so as to avoid over-blocking while maintaining child safety
- Ensure the 2025 Keeping Children Safe in Education guidance on sexual violence and harassment, including child on child sexual harassment/abuse, is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff

- Work with the Head teacher to ensure the school website meets statutory DfE requirements

Governing Body, led by Online Safety / Safeguarding Link Governor – Mr M Reynolds

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2025):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) **Online safety in schools and colleges: Questions from the Governing Board**
- Governors should seek documented assurance that the school's filtering and monitoring meet the DfE Filtering & Monitoring Standards, including annual review evidence and a record of actions taken in response to monitoring alerts
- "Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and head teacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- Governors will request evidence of staff training completion and how online-safety CPD is recorded
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and are regularly updated
- Ensure governors themselves receive briefing on online safety, filtering & monitoring and any significant incidents at least annually
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections)
- All staff will also receive online-safety training at induction and regular refresher training thereafter
- Read and follow this policy in conjunction with the school's main Child Protection policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures. All incidents will be recorded on CPOMS
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Follow the staff Acceptable use policy and Model Code of Conduct policy
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites
- For remote/homework activities involving online access, staff should select resources that are age-appropriate, provide clear parental guidance and report any concerns about platforms or apps to the DSL/OSL
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions

- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff
- Staff should ensure personal and school accounts are kept separate, avoid friending or following pupils, and report any online contact from pupils outside of school promptly to the DSL

PSHE / R(S)E /Health Education Lead/s – Miss E. Richardson/Mr J. Heeley

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Curriculum planning will be mapped explicitly to the UKCIS 'Education for a Connected World' framework so that progression of knowledge and skills is clear from EYFS to Year 6
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RE / RSE

Computing Curriculum Lead – Mr A. Wignall

Key responsibilities:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for IT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

- Ensure schemes of learning show clear reference to online-safety learning objectives (e.g., digital resilience, privacy, misinformation, AI awareness) and how these will be assessed

Subject Leaders

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Consider how the Online safety curriculum followed by Monksdown (UKCIS framework Education for a Connected World) can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

Network Manager/technician – Mersey Grid Limited

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Keep up to date with the school’s online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain a change-control log for filtering rules and system configuration changes; provide regular (e.g., termly) summaries of alerts/logs to the DSL and SLT and immediate alerts for any safeguarding concerns
- Support and advise on the implementation of ‘appropriate filtering and monitoring’ as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school’s online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school’s systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious

attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

Data Protection Officer (DPO) – Ms Needham

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
  - GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.
- The DPO will advise on DPIAs for new monitoring/filtering tools and for major third-party platforms; advise on retention policy for monitoring logs, incident records and safeguarding evidence; and support lawful sharing of data for safeguarding purposes

Context

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise and promote the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

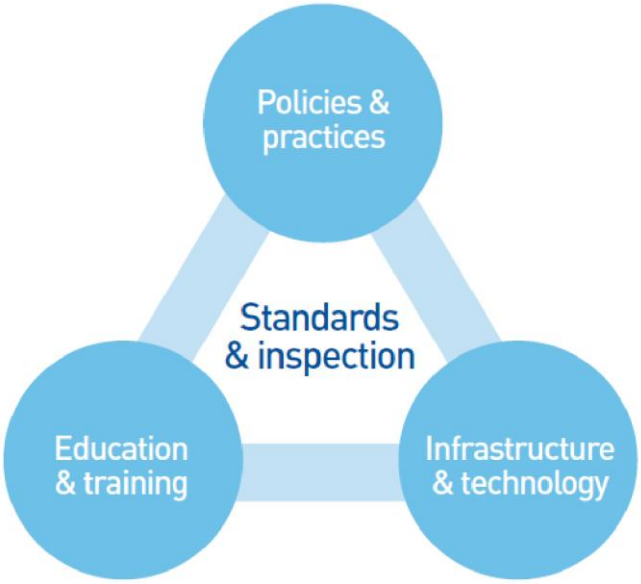
- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Online-bullying

- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

The school will also maintain awareness and undertake risk assessments for emerging digital risks such as the use/misuse of generative AI tools, deepfakes, rapidly changing social media platforms and any technologies which enable covert sharing or manipulation of images and data

The school have adopted the PIES model which is the basis of its approach towards online safety and helps to manage and minimise its risk.



Policy & Practise

The online safety policy outlines the importance of ICT within and outside of education. It provides guidance on the school's approach to online safety and details a code of conduct for school staff and pupils. The policy aims to provide an agreed, coordinated and consistent approach to online safety. The code of conduct forms the basis of the schools expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

Infrastructure and Technology

The school's educational network and access to the internet is provided by MGL through its IT partner MGL Limited. This network provides a safe and secure 30 Mbps broadband connection to the internet via the BT data centres. There is a multi-layer security shield that provides dual-layer firewall protection, intruder detection/prevention, load balancing, content caching, data traffic analysis and virus protection. There is a client-based filtering system, Smoothwall, which filters internet content using an industry base policy. Smoothwall undertakes live scanning of all sites and blocks any threats or inappropriate websites. The infrastructure has been designed to minimise the risk of; users accessing inappropriate material, data being lost or accessed by unauthorised users, virus or malware threats. All internet and network activity is logged via the Smoothwall client system and can be retrieved if required in the event of an investigation.

The school's Smoothwall configuration will be subject to regular review by the Network Manager, DSL and SLT. Review records will include a log of filter changes, rationale for allow/deny decisions, and evidence of any follow-up actions taken. The DSL/OSL will receive and review safeguarding-related alerts from the monitoring system and ensure appropriate escalation.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible.

Education and Training

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. The school is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an online safety curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

All staff receive online-safety training at induction, including clear guidance on how to report online incidents, the use of the school's monitoring tools, and their responsibilities. Training is refreshed at least annually. DSLs and technical staff attend specialist briefings to understand filtering and monitoring outputs and DPIA implications.

Our curriculum includes discrete teaching of online safety in each year group from Year 1. Foundation stage will learn about online safety through play and talk with adults as well as stories. We also have various resources including use of CEOP's thinkuknow website for both Key Stages to ensure pupil safety and wellbeing. We have a program of regular assemblies and communications to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

The school maps online-safety learning objectives to the UKCIS 'Education for a Connected World' framework to ensure progression from EYFS through KS1 and KS2. This includes age-appropriate coverage of privacy, consent, online relationships, bullying, misinformation, digital footprint, and basic awareness of AI-generated content.

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Health Education, Relationships Education
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Monksdown, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework ‘Education for a Connected World’ from UKCIS (the UK Council for Internet Safety). This document provides graduated statements for different age groups, however as staff we aim to adapt our teaching appropriately when and if an opportunity to educate our pupils in online safety arises.

Annual reviews of curriculum plans/schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Reference is also made to online safety in the annual 175 audit and through Ofsted inspections.

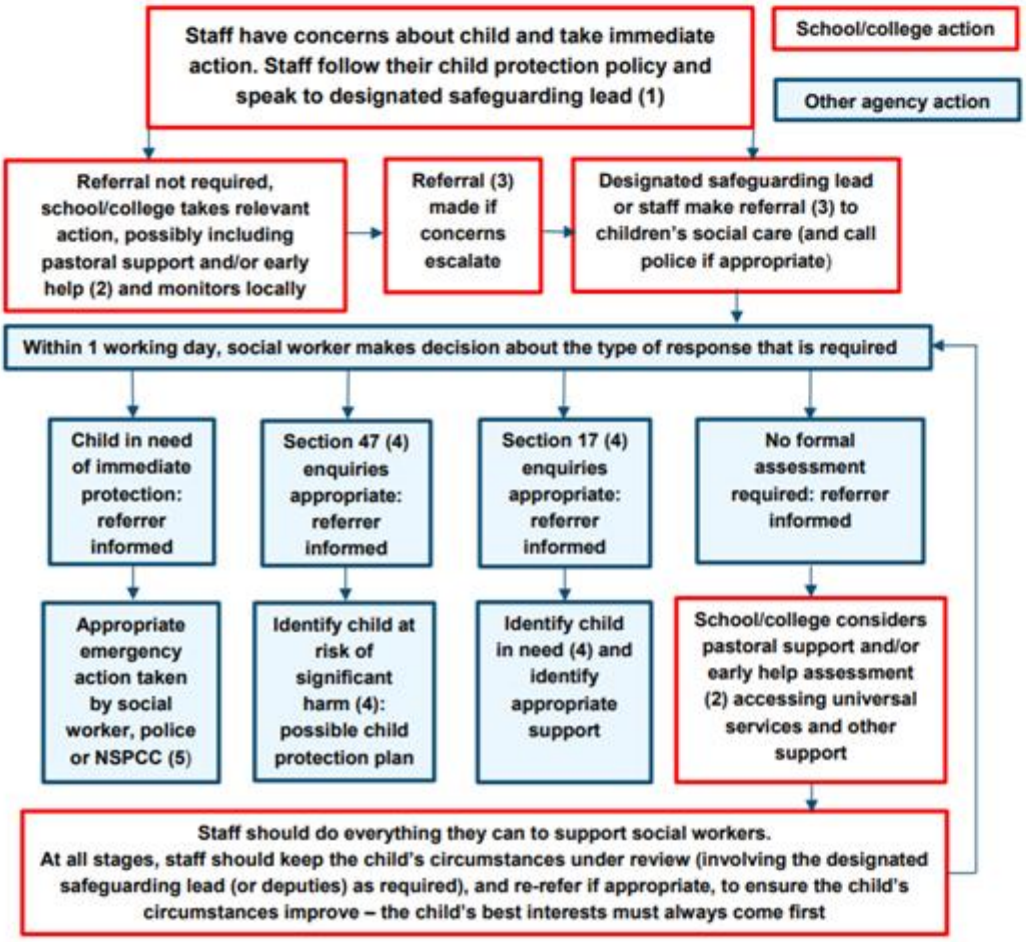
Whilst the PIES model forms the basis of the schools approach to Online safety the school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised.

The school will run regular information sessions for parents/carers on online-safety topics (including password hygiene, privacy settings, and how to support children with homework that requires online research). The school will provide guidance for parents about emerging risks (including AI tools and new apps).

As part of the Online safety policy the school will also manage:

- Sexting
- Data protection
- School website
- Incidents of misuse
- Sexual Violence/Harassment
- Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2025 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead (1)
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help (2) and monitors locally
Referral (3) made if concerns escalate
Designated safeguarding lead or staff make referral (3) to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47 (4) enquiries appropriate: referrer informed
Section 17 (4) enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC (5)
Identify child at risk of significant harm (4): possible child protection plan
Identify child in need (4) and identify appropriate support
School/college considers pastoral support and/or early help assessment (2) accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

(5) This could include applying for an Emergency Protection Order (EPO).

Sexting

The term ‘sexting’ describes the use of technology to share personal sexual content. It’s a word-mix of sex and texting. Other nicknames you may hear might be ‘cybersexing’, ‘doxing’ or ‘selfie’.

The content can vary, from text messages to images of partial nudity to sexual images or video. This content is usually created to be sent to a partner, but can be between groups and can use a range of mobile devices, technologies and online spaces. Photos and videos are often created via webcam or smartphone/tablet camera, and are shared on social networking sites such as Facebook, Twitter, Tiktok, Snapchat, Instagram, Flickr and video sites such as YouTube.

Sharing photos and videos online is part of daily life for many people, enabling them to share their experiences, connect with friends and record their lives. This increase in the speed and ease of sharing imagery has brought concerns about young people producing and sharing sexual imagery of themselves. This can expose them to risks, particularly if the imagery is shared further, including embarrassment, bullying and increased vulnerability to sexual exploitation. Producing and sharing sexual images of under 18s is illegal.

Although the production of such imagery is more than likely to take place outside of school we need to be able to respond swiftly and confidently to ensure that all children are safeguarded, supported and educated. These procedures are part of the school’s safeguarding arrangements and all incidents of youth produced sexual imagery will be dealt with as safeguarding concerns and will be responded to in line with the school’s safeguarding and child protection policy.

At Monksdown, we refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as ‘youth produced sexual imagery’) in schools. We use the UKCIS flowchart and guidance as the operational basis for our response and ensure DSLs are familiar with the process for risk assessment and referral.

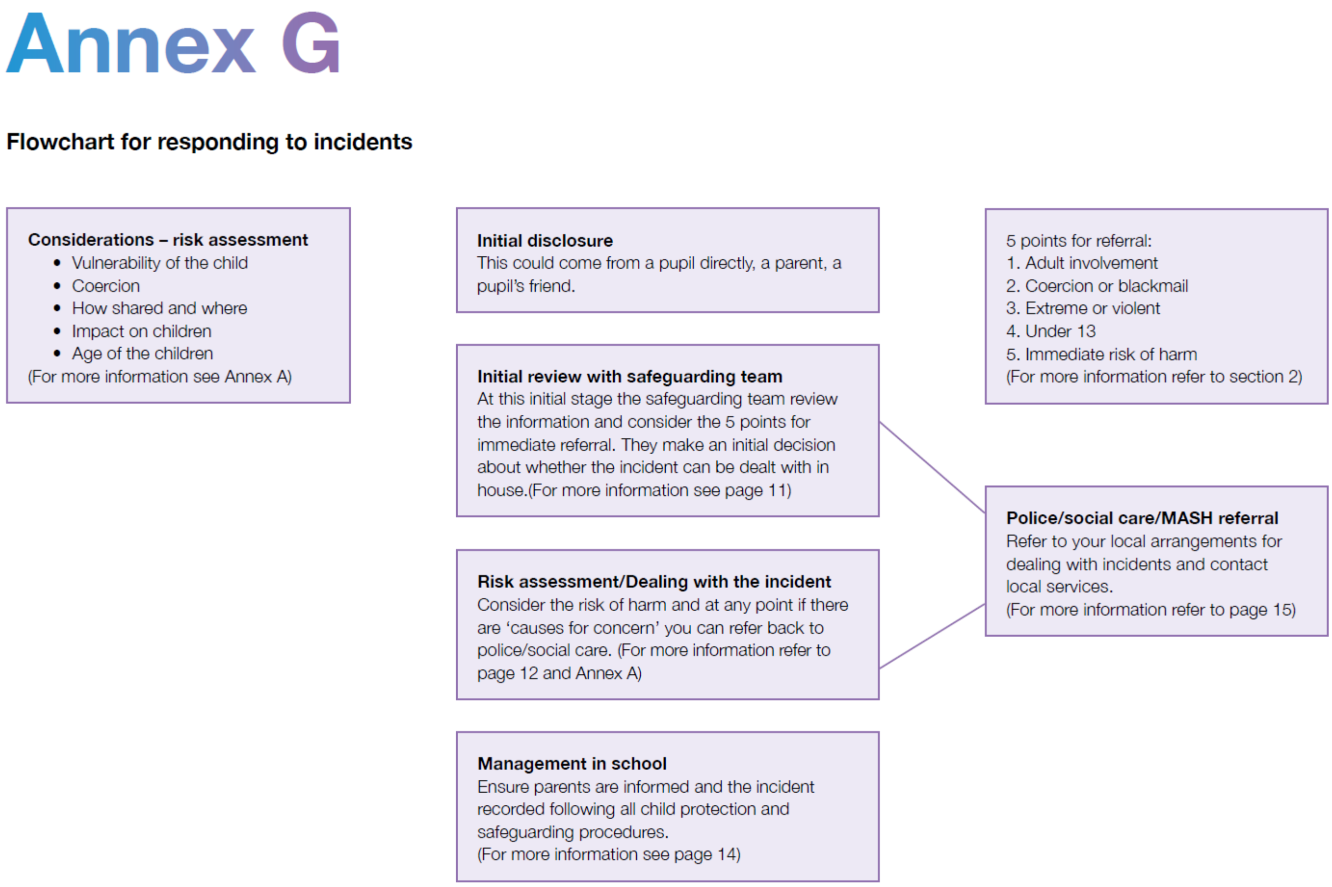
Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

Monksdown DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved. It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Where images are shared on devices or platforms, staff must not try to delete or share them; instead refer immediately to DSL who will follow UKCIS guidance and liaise with the police/children’s social care where appropriate. Any viewing of images by DSLs must be proportionate, only undertaken when strictly necessary and in line with UKCIS guidance and DfE advice; records of decisions and actions must be retained securely.

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.



Annex G

Flowchart for responding to incidents

Considerations – risk assessment

- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

(For more information see Annex A)

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 11)

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 12 and 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)

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)

Police/social care/MASH referral
Refer to your local arrangements for dealing with incidents and contact local services.
(For more information refer to page 15)

The school recognises that sexual harassment and violence can occur online. Responses will follow KCSIE 2025 guidance on child-on-child abuse; support will be offered to victims and proportionate action taken against perpetrators, including involvement of external agencies where required.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

The Acceptable Use Policies (AUPs) will explicitly cover remote access, BYOD, social media conduct, use of AI tools in schoolwork, and requirements for secure passwords and device settings. The AUP for staff includes guidance on private accounts, imagery, and interactions with pupils online.

Searching and confiscation

In line with the DfE guidance ‘Searching, screening and confiscation: advice for schools’, the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

When searching digital devices staff will act in accordance with DfE guidance (Searching, screening and confiscation) and child protection procedures. If content that is potentially illegal is discovered, the device will be secured and the police contacted; the DSL and DPO will be informed. Records of searches will be kept.

Data Protection and Data Security

“GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, **appropriate organisational and technical safeguards should still be in place […]** Remember, **the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding**.”

All pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements, which can be found on the school website.

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. See Data Protection Policy for further details.

The school will: (a) carry out DPIAs where monitoring or new third-party services are introduced; (b) maintain a documented retention schedule for monitoring logs and safeguarding evidence in consultation with the DPO; (c) ensure privacy notices reflect monitoring practices where required; and (d) ensure that information sharing for safeguarding is always prioritised and recorded in line with KCSIE.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place and not be able to access harmful or inappropriate material whilst being careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.” [DfE Filtering & Monitoring Standards]

At this school, the internet connection is provided by MGL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called Smoothwall, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

The school’s filtering and monitoring provision is reviewed at least annually (and following major changes, incidents or the introduction of new devices or platforms). Reviews include an assessment of whether the filter is blocking legitimate educational content (over-blocking) and whether monitoring thresholds are appropriate.

The DSL/OSL receives regular reports from Smoothwall (or equivalent) and will review safeguarding-related alerts; the Network Manager will provide termly summaries of logs to SLT. Any safeguarding-related alerts that meet the school’s threshold for concern will be escalated immediately via the school's safeguarding procedures.

The school maintains a change-control and audit log for filter rule changes and approvals; decisions to alter filtering are documented and available for governors' review.

Monitoring will be proportionate, respect staff and pupil privacy in line with Data Protection legislation, and be supported by DPIAs where required.

The school balances filtering rules to avoid over-blocking of curriculum-relevant content, and will provide mechanisms for staff to request temporary access for educational use where necessary (requests are logged and subject to approval).

Physical supervision (adult oversight) remains a core safeguard: technology monitoring does not replace effective teacher supervision and pastoral support.

he monitoring approach covers on-site devices and accounts; for remote/home use the school will provide guidance and recommend parental controls but cannot fully filter personal home Wi-Fi; the school will, however, set expectations in AUPs for remote learning tasks and advise parents on safer setups.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Head teacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Mr J. Heeley and Miss C. Grice. The site is hosted by Clarity.

The Department for Education has determined information which must be available on a school website.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with Mrs. L. Dickson.
- Where pupils' work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

- Consent processes for pupil images and work are recorded and reviewed annually; pupils’ images are stored and used in accordance with the Data Protection Policy and parental permissions.

Development/Reviewing

This online safety policy has been developed by a group at Monksdown Primary School and approved by:

- School Online Safety Lead
- Head Teacher and SLT
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- INSET Day training for staff
- INSET Day training for parents/carers
- *Governors meeting*
- *Parents evening*
- *School website / newsletters*
- *Digital Leader groups*

This policy and the school’s approach to filtering & monitoring will be reviewed annually and after any significant online safeguarding incident. The review will be documented and evidence provided to governors.

Should serious online safety incidents take place involving children, the following external persons / agencies should be informed:	SIL Safeguarding Team: Nicky Noon, Gisette Murphy, Maria Needham

	Email SILsafeguarding@siliverpool.gov.uk and Merseyside Police For serious incidents involving an adult in school contact the above and LADO Pauline Trubshaw, **LADO**: **Tel**: 0784 172 7309. All referrals should be sent by **email** to the **LADO** at **lado@liverpool**.gov.uk..