Online Safety Policy

Policy number	14	Person responsible	DD
Date created	April 26	Review date	April 27
Signed		Date	21/4/26

Table of Contents

Scope of the Online Safety Policy

This Online Safety Policy sets out how Oakwood Education will safeguard members of our community online, in line with statutory guidance and best practice. The setting is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of our community who access or use school digital systems, including staff, learners, volunteers, parents/carers and visitors. It applies to use of Oakwood systems both on and off site, and to the use of personal devices on the site (where permitted).

Where online safety concerns or incidents occur outside of the setting and are known to the provision, Oakwood Education will respond in line with this policy and related procedures, including the setting's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of the provision.

Policy and leadership

Responsibilities

Online safety is a shared responsibility. All members of our community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Directors and senior staff

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the setting meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff.
- Ensure that the relevant colleagues are trained and able to fulfil their roles.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Work with the DSL and IT provider on filtering and monitoring.

Designated Safeguarding Lead (DSL)

KCSIE states the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes.

The DSL will:

- Lead safeguarding, including online safety
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information, confirming at least annual checks.
- Ensure appropriate support for learners with SEND.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only setting-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

Learners

Learners will:

- Follow the Learner AUA and Online Safety Policy (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-provision behaviour may be addressed where it affects our community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

Oakwood Education will:

- Publish the Online Safety Policy and share the learner AUA

- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices.

Online Safety Group

The Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice.

Membership *(amend as appropriate)*

- Director
- DSL
- IT/technical representative (provider)

Core responsibilities

The group supports the DSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Gather feedback from learners, staff and parents/carers and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.

Policy

Online Safety Policy

The Online Safety Policy is part of the provision's safeguarding framework and should be read alongside Safeguarding/Child Protection, Behaviour, Anti-Bullying and Data Protection policies.

What the policy does

- Defines responsibilities for online safety.

- Sets expectations for safe, professional and ethical use of technology (including AI).
- Sets out reporting, recording and response procedures for online safety incidents.
- Supports compliance with KCSIE, DfE Technical Standards and UK GDPR.
- Promotes learners' digital competence and critical understanding.

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually, and sooner if risks/technology change.
- Monitored by the DSL using anonymised incident trends, filtering/monitoring reports and education review activity
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training.
- Communicated to learners and parents/carers through AUAs and awareness activity.

Acceptable use

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs). AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

- staff and learner induction
- posters in areas where technology is used
- curriculum and awareness sessions
- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) • *Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).*					X
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (e.g., denial of service)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	• Using penetration-testing tools without explicit permission					
Unacceptable (not illegal) under setting policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

The statements below are related to non-engagement or educational purposes. Where a learner/member of staff needs to access gaming/shopping etc for provision purposes this is allowed and agreed in advance.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (*e.g. Roblox, Fortnite, Minecraft*)	X				X			
Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)*	X				X			
Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*)	X				X			
Social media and user-generated platforms *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services*	X				X			
Messaging, chat and voice *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)*	X				X			
Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify*	X				X			
Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)*	X				X			

Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds)*			X				X	
Mobile phones used for learning (teacher-directed and supervised)			X				X	
Mobile phones used during social time/breaks (where permitted) including device-free approaches			X				X	
Taking photos/video/audio on devices (including sharing, location data and consent)	X				X			
Other personal devices *(e.g., tablets, handheld consoles, VR headsets, wearables)*			X				X	
Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)*			X				X	
School email used for personal communication (non-work/non-learning)	X				X			
Unapproved AI tools/services *(generative AI chatbots and image/video tools, AI companions, browser extensions)*	X				X			

Acceptable/Unacceptable Actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
	the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Reporting and responding

Introduction

The setting is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the provision recognises that online risks may occur in the setting or outside and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

Oakwood Education recognises national findings, including the Ofsted *Review of Sexual Abuse in Schools and Colleges* (2021), which highlight that children may not always feel able to report. The provision assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns.

Reporting Concerns

The setting will ensure that:

- Clear, accessible reporting routes are in place for all members of our community, including pupils, staff, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools, email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the provision website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

Oakwood Education will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods

- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring

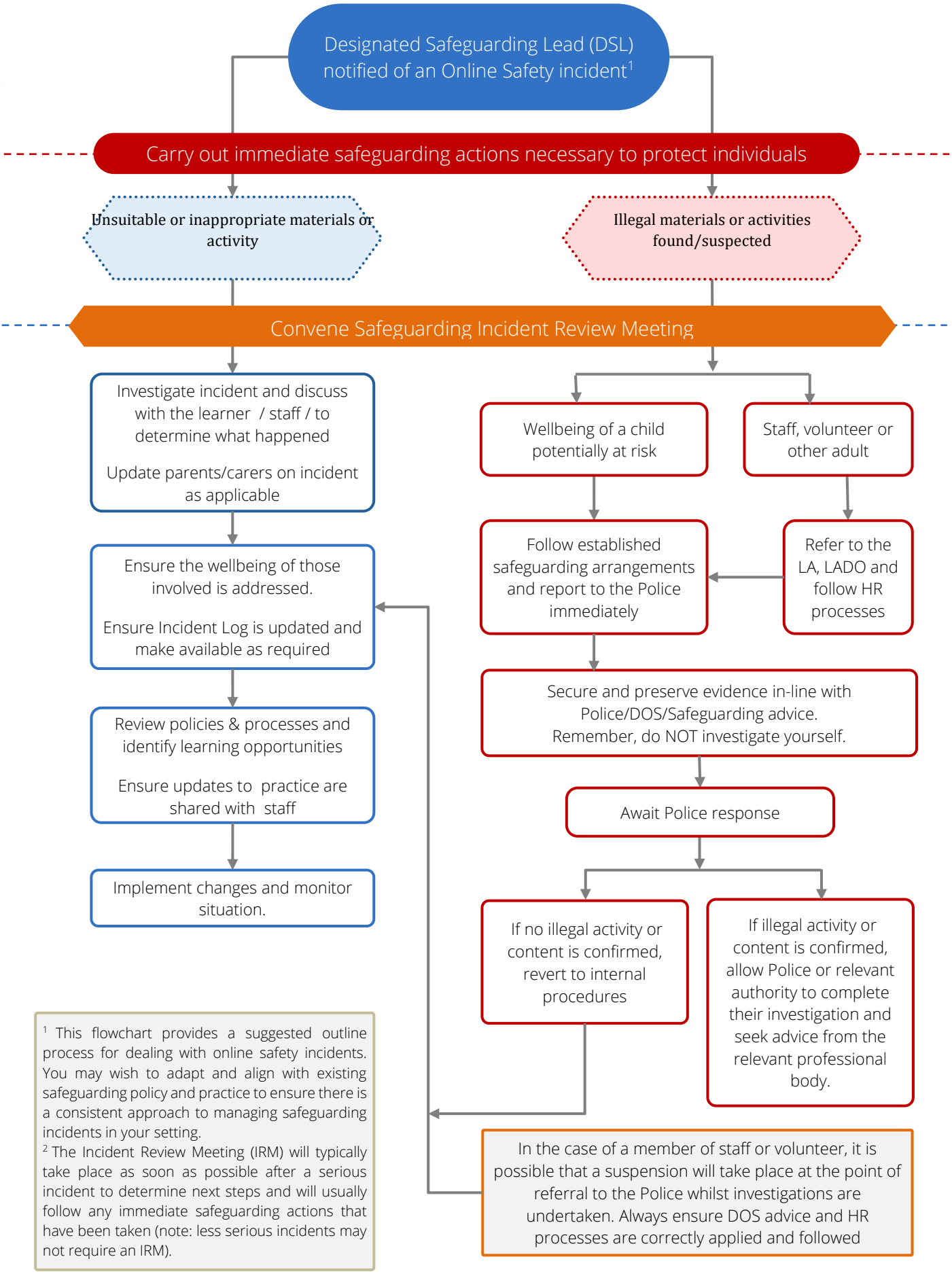
Oakwood Education will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
    - The Online Safety Group
    - Senior leaders
    - *Staff*
    - *Learners, where appropriate*
    - *Parents/carers through general communications*
    - *Local safeguarding partners where relevant*

External Support and Escalation

The school will work with appropriate external agencies when required, including:

- Local Authority safeguarding teams
- Local Authority Designated Officer (LADO)
- Police / CEOP
- Local Safeguarding Partnership guidance (e.g., harmful sexual behaviour support)
- *UK Safer Internet Centre's Professionals Online Safety Helpline*
- *Reporting Harmful Content service*



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Responding to Learner Actions

Incidents	Refer to tutor	Refer to DSL	Refer to SLT	Refer to Police/Social Services	Refer to IT Services Provider	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X	X	X			
Unauthorised access to the school network, including using another person's account or sharing usernames/passwords.	X		X		X				
Damaging, corrupting or deleting another user's data.	X		X		X	X			
Sending offensive, harassing or bullying emails, texts or messages.	X	x	X		X	X			
Unauthorised downloading/uploading, file sharing or distribution of files.	X		X		X	X			
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).	X	X	X		X				
Failing to report accidental access to offensive or pornographic material	X	X	X			X			
Deliberately accessing offensive or pornographic material (or attempting to)	X	X	X		X	X			
Sharing or receiving content that breaches copyright or data protection law.	X		X		X				
Unauthorised use of devices, including taking photos/videos or audio recordings.	x	x	X		X	X			

Unauthorised use of online services (apps, websites or platforms).	X	X	X		X	X			
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	X		X		X	X			
Repeated breaches of these rules following previous warnings or sanctions.	X		x		x	X			

Responding to Staff Actions

Incidents	Refer to line manager	Refer to SLT / Director	Refer to Police / LADO	Refer to IT Services Provider	Issue a warning	Further Disciplinary action in line with Behaviour Policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X		X
Breaching data protection or cyber-security requirements, including network security rules.		X		X	X	
Accessing offensive or pornographic material (or attempting to).		X	X	X		X
Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software.		X		X		X
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).	X	X		X		X
Unauthorised downloading, uploading or file sharing.	X	X		X		X
Breaching copyright, licensing or intellectual property, including misuse of AI systems.	X	X		X	X	
Unauthorised account/network access, including sharing passwords, using another person's account, or allowing others access.		X		X	X	
Sending offensive, harassing or bullying emails, texts or messages.		X		X		X

Use of personal email/social media/messaging to communicate with learners or parents/carers.		X	X	X		X
Inappropriate personal use of school technology, including personal email and social media use during work time/using school systems.		X	X	X		X
Mishandling personal data, including storing, displaying or transferring it insecurely.	X	X		X	X	
Any action that undermines professional conduct or a staff member's professional standing.	X	X			X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X			X	
Failing to report incidents, whether accidental or deliberate.	X	X			X	
Repeated breaches following previous warnings or sanctions.	X	X				X

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In educational provisions, AI is typically used in three areas: learner support, teacher support, and setting operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

Policy statements

Oakwood Education will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.

- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

Oakwood Education will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only setting-approved AI tools may be used for work, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

Oakwood Edcucation will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The setting will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The setting will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in further disciplinary action.

Education

Online Safety Education Programme

Online safety education is a core part of the setting's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

As needed/required, Oakwood Education delivers a planned, progressive and inclusive programme of online safety education to learners, aligned to nationally recognised guidance and frameworks. Learning is age-appropriate, builds on prior learning and is matched to need.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Staff

In line with DfE Keeping Children Safe in Education (KCSIE), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the provision's safeguarding approach, wider staff development and curriculum planning.

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include (select/delete as appropriate):

- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/OSL (or nominated staff) to individuals as required.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks, and that many external bodies can enhance the school's safeguarding approach. The provision therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the setting's engagement with external stakeholders:

Working with Parents and Carers

Oakwood Education will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the provision website, learning platforms, and digital communication tools.
- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources (e.g. UK Safer Internet Centre, Internet Matters, Childnet, SWGfL).

- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant policies related to online safety.

Wider Community and Agencies

Oakwood Education recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice, including through recommended tools such as 360 Early Years or 360 Groups.

Technology

Purpose

The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Filtering and Monitoring

The setting has appropriate systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance.

The provision ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed

- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all provision-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated

Oversight and Review

- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Technical Security

The provision takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

Oakwood Education ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The provision recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents.

Oakwood Education ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats

- senior leaders understand cyber risks and receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Data Protection

Oakwood Education is committed to protecting personal data and complying with data protection legislation.

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration.

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

Technology Practice

Purpose

The provision recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in *Keeping Children Safe in Education*, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice and education.

Device Management

The provision manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education

Oakwood Education ensures that:

- expectations for the use of provision-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on the premises or systems

Decisions about device use are informed by risk assessment and reviewed regularly.

Digital Content

The provision recognises that digital content (images, video and any other multi-modal digital media) can enrich learning and communication when used responsibly. It directly supports KCSIE expectations around sexual imagery, sharing of images, consent and coercion. It also reinforces lawful management of digital content as part of safeguarding and embeds education and prevention alongside policy.

Oakwood Education ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The provision uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency.

Oakwood Education ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the provision are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- online safety information is shared with parents, carers and the wider community
- staff understand expectations around professional conduct and online behaviour

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, learners and parents
- national guidance and statutory expectations

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, learners and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes (e.g. using ProjectEVOLVE Knowledge Maps assessment and tracking). Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.

- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety

List of appendices

A1 - Learner Acceptable Use Agreement Template – for older learners
A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
A8 - Harmful Sexual Behaviour Policy Template
C1 – Filtering and Monitoring Policy Template

Appendix A1 - Learner Acceptable Use Agreement Template

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their online safety policy and other relevant school policies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

Learner Acceptable Use Agreement Form

I agree to use the school's digital systems responsibly to protect my safety, the security of the school systems, and others.

Personal Safety

- The school will monitor my use of its digital systems, devices, and communications.
- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.
- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.
-

Respecting Others' Work and Information

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.

- I will only use Artificial Intelligence (AI) tools approved by the school and ensure my use is ethical, legal, and transparent.
- I will fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- I will avoid downloading or using copyrighted or protected materials without proper permissions.

Responsible Online Behaviour

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not bully, harass, threaten, upset or make fun of others.
- I will only use platforms or software approved by the school and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand cybersecurity poses a risk to both me, other learners and the school and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the age requirements for social media, apps, and tools.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of the school, its staff, and other learners.
- I will ensure my behaviour reflects positively on the school, both in and out of school settings.
- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, learners in embarrassing situations or the setting up of fake accounts.

Consequences of Misuse

- I understand that failing to follow this agreement may lead to consequences, including loss of access to the school's systems, detentions, suspensions, contacting parents/carers, or involvement of the police in serious cases.

By following these guidelines, I will contribute to a safe, respectful, and productive online environment.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)

- I use my own devices in the school (when allowed)
- I use digital technologies out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

(Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware of acceptable use through education programmes/awareness raising).

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carer acceptable use agreement (see template later in this document). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement Template

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies.

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people , both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies. .

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
  - will only use AI technologies approved by the school
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
  - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
  - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance

    - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
    - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using digital technologies in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

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

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix A8 - Harmful Sexual Behaviour Policy Template

Purpose

The school recognises that harmful sexual behaviour may be happening but not reported and that it increasingly occurs online involving image sharing, coercion, exploitation and anonymous abuse.

The purpose of this policy is to set out the school's approach to preventing, identifying and responding to Harmful Sexual Behaviour (HSB), sexual harassment and sexual violence between children.

This policy forms part of the school's safeguarding framework and should be read alongside other relevant policies.

The school adopts a zero-tolerance approach to harmful sexual behaviour in line with national safeguarding guidance (see list below)

Scope

This policy applies to:

- All learners, staff, volunteers and governors
- Behaviour occurring within and outside school where it impacts the school community

Legislative and National Context

This policy reflects national guidance including:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children (DfE)
- Violence Against Women and Girls (VAWG) strategy (UK Government)
- Ofsted Review of Sexual Abuse in Schools and Colleges.
- Sharing Nudes and Semi-Nudes: Advice for Education Settings

Roles and Responsibilities

- Governors provide strategic oversight, ensure annual review of this policy and monitor safeguarding trends.
- Senior Leaders promote a culture of respect and equality and ensure consistent implementation and staff training.
- The Designated Safeguarding Lead (DSL) leads responses to incidents, ensures safeguarding procedures are followed, completes risk assessments and liaises with external agencies.
- All staff must challenge inappropriate behaviour, report concerns immediately to the DSL and respond to disclosures in a calm and supportive manner.

Policy Statement

The school will ensure that:

- A whole-school safeguarding approach is taken to preventing harmful sexual behaviour
- All reports are taken seriously and responded to promptly
- Victims are supported, believed and protected
- Children displaying harmful behaviour receive appropriate safeguarding and educational support
- Incidents are managed in line with safeguarding and statutory procedures
- Patterns and trends are monitored to inform prevention strategies

Prevention and Education

The school will ensure that:

- High-quality Relationships and Sex Education (RSE) is delivered
- Learners are taught about consent, respectful relationships and healthy boundaries
- Online safety education addresses digital sexual abuse, coercion and image-based harm
- Sexist language, misogyny and harmful gender stereotypes are actively challenged
- Learners are encouraged to be positive bystanders and report issues they see
- Reporting systems are accessible, appropriate and clearly communicated

Reporting and Responding

The school will ensure that:

- Multiple reporting routes are available and understood
- All incidents are recorded securely in line with safeguarding and data security procedures
- Risk assessments are completed where appropriate
- The safety and wellbeing of those affected is prioritised
- External specialist agencies are involved where required
- Criminal matters are referred to the police where appropriate

Support and Risk Management

The school will ensure that:

- Victims receive appropriate pastoral and safeguarding support
- Children displaying harmful behaviour receive proportionate and educational intervention
- Risk assessments are dynamic and regularly reviewed
- Supervision and safety planning are proportionate and protective

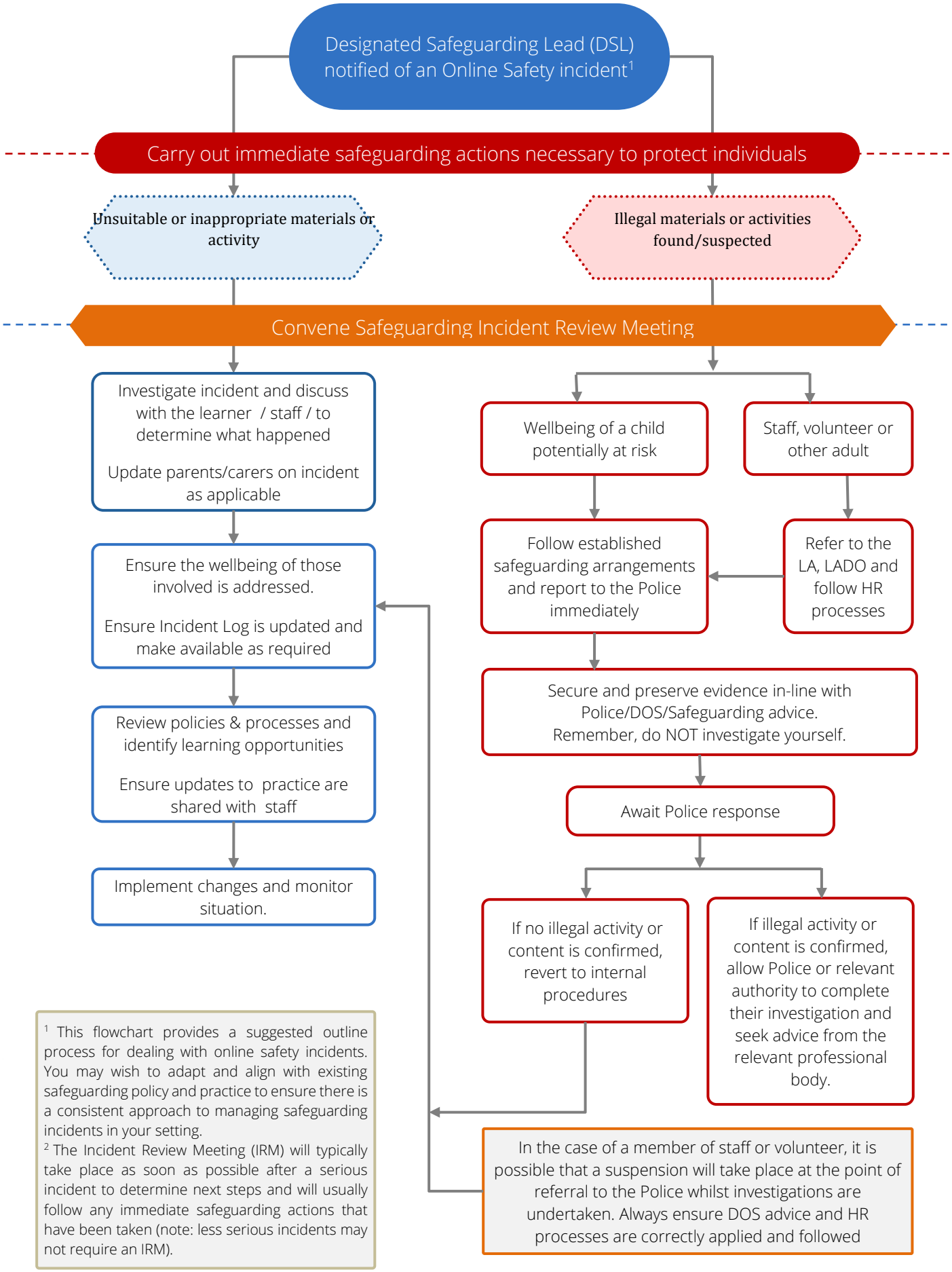
Online Harmful Sexual Behaviour

Online incidents will be managed in line with DfE guidance and may involve specialist reporting services where appropriate.

Training and Review

The school will ensure that:

- DSLs receive specialist safeguarding training
- All staff receive regular safeguarding updates



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Appendix C1 – Filtering and Monitoring Policy Template

Purpose

The purpose of this policy is to ensure that appropriate filtering and monitoring systems are in place to safeguard learners and staff from harmful or illegal online content, while enabling safe and effective teaching, learning and professional practice. Filtering and monitoring form part of the school's wider safeguarding responsibilities and are implemented in line with Keeping Children Safe in Education (KCSIE) and the DfE Filtering and Monitoring and Technical Standards.

Scope

This policy applies to:

- All users of the school's IT systems
- All school-owned devices
- Any device accessing the school's network or internet connection
- Filtering and monitoring provided through third-party or managed services

Roles and Responsibilities

- Governors provide strategic oversight and assurance that filtering and monitoring standards are met.
- Senior leaders ensure appropriate systems are in place, reviewed and resourced.
- The DSL leads safeguarding responses arising from filtering or monitoring alerts.
- The IT service provider maintains systems and provides reports as agreed.
- All staff report concerns relating to access, alerts or system effectiveness.

Policy Statement

The school will ensure that:

- Internet access is filtered to block illegal, harmful and inappropriate content
- Monitoring systems are in place to identify safeguarding concerns and enable timely intervention
- Filtering and monitoring are proportionate, transparent and risk-based
- Roles and responsibilities are clearly defined and understood
- Provision is reviewed regularly and improved in response to risk, practice and guidance

Filtering and monitoring are recognised as supporting safeguarding, not replacing education, supervision or professional judgement.

Filtering

The school will ensure that filtering systems:

- Block access to illegal content, including child sexual abuse material, terrorist material and other unlawful content
- Manage inappropriate and/or harmful content (including search terms and results). These may include:
    - Gambling
    - Hate speech/discrimination
    - Harmful content
    - Mis/Disinformation
    - Piracy and copyright theft
    - Pornography
    - Self-harm and eating disorders
    - Violence against women and girls
- Are age-appropriate and suitable for an educational environment
- Are applied consistently to all users, devices and internet connections, including backup connections
- Allow the identification of individual users and devices in the event of breaches of the filtering policy
- No user should be able to deactivate or bypass systems that filter illegal content.
- Prevent circumvention through VPNs, proxy services or similar technologies
- Support differentiated access for different user groups (e.g. staff and learners)
- Are reviewed regularly to avoid inappropriate over-blocking that may restrict teaching and learning

The school understands the capabilities and limitations of the system and potential impact on implementation and policy is understood.

The school will use recognised tools and guidance to assure the effectiveness of filtering provision e.g., testfiltering.com

Monitoring

The school will ensure that monitoring:

- Enables the identification of safeguarding concerns in a timely manner
- Uses a combination of physical supervision, manual checks and technical systems as appropriate
- Generates alerts that can be prioritised and acted upon by trained staff
- Is subject to human review and professional judgement
- Is clearly communicated to users through policy and acceptable use agreements

Monitoring should be proportionate to the school's risk profile and should not create a culture of surveillance.

Review and Training

Filtering and monitoring provision should be reviewed at least annually and whenever risks or technologies change. Staff, governors and those with specific responsibilities will receive appropriate training.