

Taywood Nursery School and Seedlings

Online Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Date created: April 2025

Next review date: April 2026

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Taywood Nursery School and Seedlings to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Taywood Nursery School and Seedlings will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the <i>school governing body</i> on:	<i>14th May 2025</i>
The implementation of this Online Safety Policy will be monitored by:	<i>Jennifer Slater- Headteacher/ DSL and Claire Farr (DSL)</i> <i>Suzanne Smith- Safeguarding Governor</i>
Monitoring will take place at regular intervals:	<i>Annually and in response to statutory changes</i>
The <i>governing body</i> will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	<i>Termly feedback to Safeguarding Governor</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>April 2026</i>

Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>Local Authority Designated Officer (LADO)</i> <i>Police</i>
--	---

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *internal monitoring data for network activity*
- *discussions with*
 - *children*
 - *parents and carers*
 - *staff.*

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals¹ and groups within the school.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff².

- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher will carry out the internal online safety monitoring role.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the safeguarding governor, Suzanne Smith, who will receive regular information about online safety incidents and monitoring reports. The safeguarding governor will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant governors
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups

- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead (this is the Headteacher and DSL at Taywood Nursery School and Seedlings)

The Online Safety Lead will:

- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers
- liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)

Curriculum Leads (this is the Headteacher/ DSL at Taywood Nursery School and Seedlings)

Curriculum will ensure that children have:

- a discrete, age- appropriate programme
- PHSE programmes
- A mapped cross-curricular programme

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level *and* only carried out using official school systems and devices (where staff

use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements

- they immediately report any suspected misuse or problem to the DSLs for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned children are exposed only to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Provider

In accordance with the DfE Filtering and Monitoring Standards, the DSL will work closely with the UT service provider to meet the needs of our school. The IT provider has responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

"The IT service provider will work with the DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Lancashire Digital Services for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

Children

- should know who to talk to as a trusted adult for any issues related to online safety
- should understand that they should check with an adult before accessing online material

Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to children in school.

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Online Safety Policy

The DfE guidance “Keeping Children Safe in Education” states:

“Online safety and the school or college’s approach to it should be reflected in the child protection policy”

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through the Staff Handbook, as well as shared at INSET and staff training
- is published on the school website

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- registration and induction process for children
- staff induction and handbook
- communication with parents/carers (signed at induction)
- as part of the curriculum on digital safety
- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	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:	<p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • 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 <p>N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges</p>					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> 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) <p>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 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</p>					X
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	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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	

AGREED USAGE BY STAFF, OTHER ADULTS, INCLUDING VISITORS AND CHILDREN	
Online gaming	NOT ALLOWED BY STAFF, OTHER ADULTS OR CHILDREN
Online shopping/commerce	ALLOWED FOR SELECTED STAFF ONLY (OFFICE AND SLT)
File sharing	ALLOWED BY STAFF
Social media	ALLOWED BY SLT AND OFFICE STAFF
Messaging/chat	ALLOWED BY STAFF USING SCHOOL PLATFORMS ONLY

Entertainment streaming e.g. Netflix, Disney+	NOT ALLOWED BY STAFF, OTHER ADULTS OR CHILDREN
Use of video broadcasting, e.g. YouTube, Twitch, TikTok	ALLOWED BY STAFF ONLY USING YOUTUBE KIDS ON SCHOOL DEVICES ONLY
Mobile phones may be brought to school	ALLOWED BY STAFF AND OTHER ADULTS (NOT PERMITTED IN CLASSROOMS)
Use of mobile phones for learning at school	NOT ALLOWED BY STAFF, OTHER ADULTS AND CHILDREN
Use of mobile phones in social time at school	ALLOWED BY STAFF AND OTHER ADULTS IN DESIGNATED SPACE (STAFF ROOM AND OFFICE)
Taking photos on mobile phones/cameras	NOT ALLOWED BY STAFF, OTHER ADULTS OR CHILDREN. SCHOOL IPADS ONLY TO BE USED
Use of other personal devices, e.g. tablets, gaming devices	ALLOWED BY STAFF ON SCHOOL DEVICES. ALLOWED BY VISITORS WITH APPROVAL FROM DSL
Use of personal e-mail in school, or on school network/wi-fi	ALLOWED IN OFFICE AND STAFF ROOM USING OWN DATA BY SCHOOL STAFF AND OTHER ADULTS. SCHOOL WIFI IS NOT TO BE USED ON PERSONAL DEVICES
Use of school e-mail for personal e-mails	NOT ALLOWED BY SCHOOL STAFF
Use of AI services that have not been approved by the school	ALLOWED BY DSL/ SLT ONLY

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.

- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff.

Reporting and responding

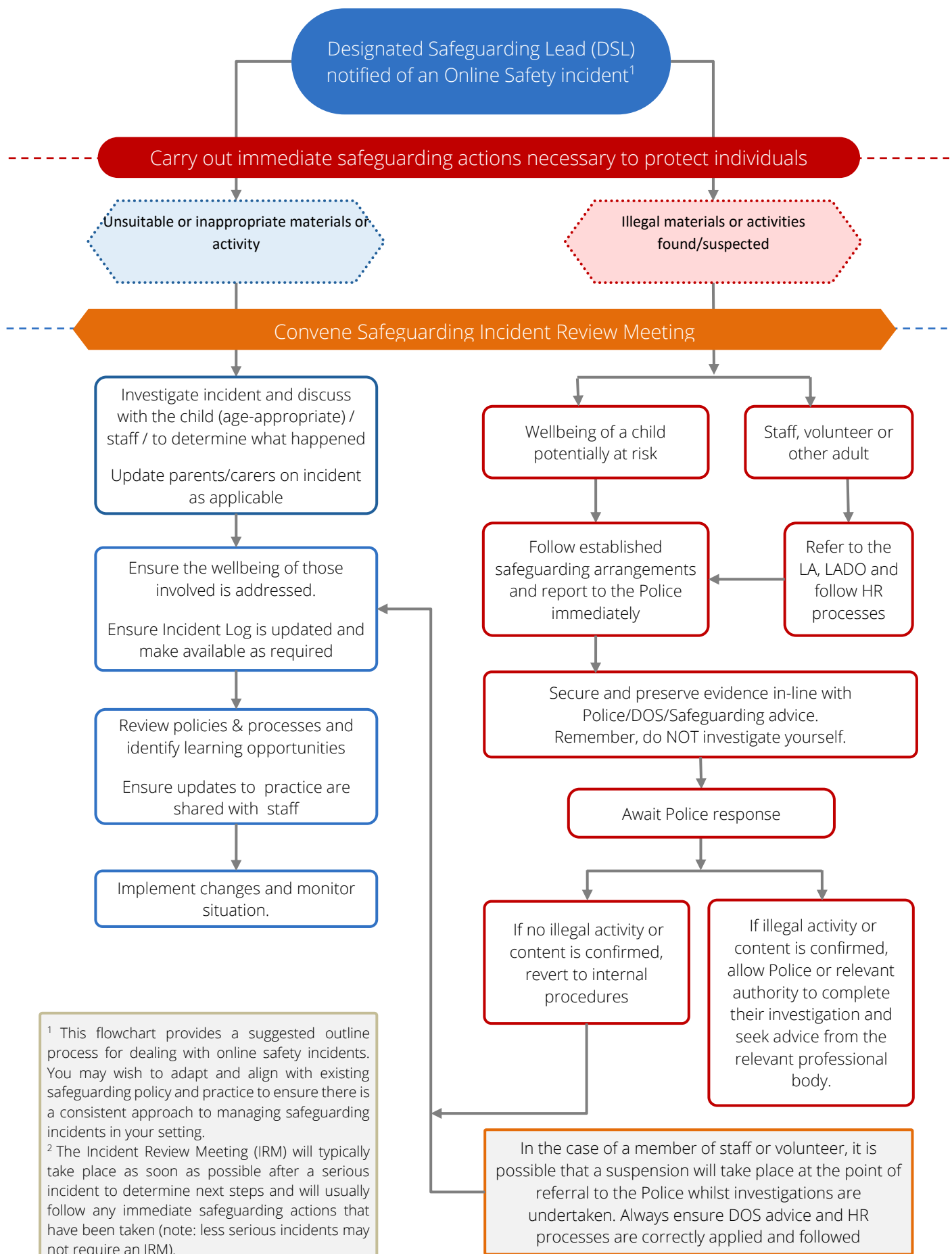
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures. Illegal activity includes:
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking offences under the Computer Misuse Act
 - Copyright theft or piracy

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by children and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
 - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - internal response or discipline procedures
 - involvement by local authority
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents are logged on the reporting incidents form
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:

- the safeguarding governor, and relevant members of SLT for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
- staff, through regular updates
- parents/carers, through newsletters, school social media, website
- full governors, through regular safeguarding updates
- local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Staff Actions

<p>The Headteacher should be informed of all incidents.</p> <p>The Headteacher will seek advice from the following professionals/ agencies, which could lead to;</p> <ul style="list-style-type: none"> • A warning being issued • Suspension • Disciplinary action
Incidents to be reported
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)
Actions which breach data protection or network / cyber-security rules.
Deliberately accessing or trying to access offensive or pornographic material
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
Using proxy sites or other means to subvert the school's filtering system.
Unauthorised downloading or uploading of files or file sharing
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner
Actions which could compromise the staff member's professional standing

Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.
Failing to report incidents whether caused by deliberate or accidental actions
Continued infringements of the above, following previous warnings or sanctions.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in , its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and children will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.

- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not 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.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- *AI tools may be used to assist teachers in the assessment of childrens' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI*
- *Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.*
- *We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.*
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Online Safety Education Programme

An online safety curriculum for nursery aged children focuses on foundational digital habits, using simple age- appropriate language and interactive activities. Children do not navigate the internet

independently, but are introduced to basic concepts of safety, kindness, adult supervision, appropriate use of screens vs other activities.

Our curriculum includes:

- Understanding technology- different types and how they are used (tablets, phones, laptops, interactive boards, digital toys, technology around the home)
- Asking for help- seeking permission before using technology, using Youtube kids, who they can speak to if they see something they don't like online
- Being kind online- including respecting and caring for property/ screens
- Screen time and balance- the effects of too much screen time, acceptable screen time e.g. interactive maths games, promoting physical/ other play over screen time
- Personal information- introducing keeping our names, addresses and faces private online

Our curriculum will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

Children are not permitted to browse the internet freely.

Youtube Kids only is permitted in class.

Staff/volunteers

The DfE guidance "Keeping Children Safe in Education" states:

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

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

- the training will be an integral part of the school's annual safeguarding, data protection and cyber-security training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- *the Designated Safeguarding Lead and Deputy DSL (or other nominated person) will receive regular updates through attendance at external training organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

Families

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

- *Curriculum overview shared*
- *letters, newsletters, website, learning platform,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers*

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in

place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice.

Filtering

- The headteacher and the safeguarding governor, are responsible for ensuring these standards are met.
- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre [Appropriate filtering](#).
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed by the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

- There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings
- *Children will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](#)*
- *the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

Monitoring

The DfE Technical Standards for Schools and Colleges states:

"Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything."

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance.

The school has monitoring systems in place (Netsweeper) to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the

responsible governor. The results of the review will be recorded and reported as relevant.

- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- Monitoring enables alerts to be matched to users and devices.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the [DfE Technical Standards for Schools and Colleges](#)

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre
- all school networks, devices and system will be protected by secure passwords
- the administrator passwords for school systems are kept in a secure place
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Joanne Clegg is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider

- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile
- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- dual-factor authentication is used for sensitive data or access outside of a trusted network
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device ³	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	No	Yes after consent is given by SLT
No network access				Yes	Yes	Yes when working independently.

School owned/provided devices:

- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.

³ Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available (staff room)
- use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

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

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

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

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- the school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies
- staff/volunteers must be aware of those children whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- childrens' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website
- Social media
- Online newsletters
- Class Dojo
- Tapestry

The school website is managed/hosted by School Spider. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where children's images or videos are published, their identities are protected, and full names are not published.

The website advises parents and the wider community to contact the headteacher by email to register issues and concerns to complement the internal reporting process.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly [what personal data is held](#), where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- provides staff and parents with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff
- ensures that where AI services are used, data privacy is prioritised

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.

- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Cyber Security (new January 2025)

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, *(in partnership with their technology support partner)*, has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school’s governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school has a business continuity and incident management plan in place following LCC guidance
- there are processes in place for the reporting of cyber incidents. All staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Taywood Nursery School and Seedlings

Acceptable Use Agreement

The statements below are shared with children when using technology.

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

Taywood Nursery School Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that children will be responsible users and stay safe while using the internet and other communications 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 parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that children have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the child-friendly acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the children in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name:

Child's Name:

As the parent/carers of the above child, I give permission for my son/daughter to have access to the digital technologies at school.

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

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

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

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

This form will be kept in paper form in the child's registration file

It will be accessed by office staff and SLT only

It will be stored in the school office for the length of time that the child attends the school

It will be safely destroyed after the child leaves the school

Signed:

Date:

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in nursery to support learning.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent's/carers' permission before taking images of members of the school. We will also ensure that when images are published that children cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

This form (electronic or printed): Printed	The images: Electronic Images of children may be displayed around the nursery school to celebrate learning. These will be destroyed when a child is taken off roll.
Who will have access to this form: SLT and office staff	Where the images may be published: Facebook, the schools website, Class Dojo, Tapestry
Where this form will be stored: School office in child's file	Who will have access to the images: All staff
How long this form will be stored for: Length of time children are at school.	Where the images will be stored: On devices
How this form will be destroyed: Shredded when the child is taken off roll.	How long the images will be stored for: Full wipe of photos at least half-termly
	How the images will be destroyed: Deleted

Digital/Video Images Permission Form

Parent/Carers Signature: Date:

Child's Name:

As the parent/carer of the above child, I agree to the school taking digital/video images of my child/children to support learning activities and in publicity that reasonably celebrates success and promotes the work of the nursery school. At Taywood Nursery School and Seedlings, this is through Facebook, on our website, Class Dojo and Tapestry.	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Taywood Nursery School Staff (and Volunteer) Acceptable

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. (They must not be written down and displayed in class.
- I will sign out/ log out of all devices.
- 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 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 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 the internet 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 a warning, a suspension, referral to Governors and/or the Local Authority 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:

Taywood Nursery School and Seedlings

Policy for Harmful Sexual Behaviour

Statement of intent

Our school has a zero-tolerance approach to any harmful sexual behaviour involving children and acknowledge that it could be occurring at Taywood Nursery School and Seedlings, and in our school community. The school is proactive in its approach to assessing prevalence, responding to incidents and challenging and changing behaviour. This policy applies to all governors, staff and children.

Schools and colleges have a statutory duty to safeguarding the children in their setting. We work together to foster an environment that creates healthy relationships for children and young people.

Our whole-school approach encourages healthy relationships and works to prevent harmful sexual behaviour. We provide high quality education within the curriculum to reduce the likelihood of the situations occurring.

We recognise that HSB is harmful to both the child/children affected by the behaviours and the child/children who displayed the behaviour and provide ongoing support for all involved.

Our approach is to treat everything as safeguarding incident in the first instance - we distinguish between behaviours that are exploratory and part of healthy age and ability appropriate development and those that may be harmful.

As a school we provide regular opportunities for school staff to understand what harmful sexual behaviours might look like and what they should do in the event of a report.

Related policies

This policy should be read in conjunction with:

- Child protection and safeguarding policy
- Whistleblowing
- Behaviour policy, referencing our anti-bullying policy
- Online safety
- Acceptable Use Agreements

Definitions

As stated in the Sexual Offences Act 2003, the term Harmful Sexual Behaviour (HSB) covers a wide range of behaviours, often these may be considered problematic, abusive, or violent and may also be developmentally inappropriate. HSB can occur online, offline or in a blend of both environments. The term HSB is widely acknowledged in child protection and should be treated in this context.

Whilst peer on peer harassment has become a widely recognised term, this is already moving towards child on child in recognition that age and development is a factor in making decisions about behaviour. A significant age difference between the children involved in an incident may lead to a decision about the behaviour being harmful or not. For example, this could be an older child's behaviour towards a pre-pubescent child, or a younger child's behaviour towards an older child with learning difficulties. It is important that Designated Safeguarding Leads (DSL) know what is and is not HSB. DSLs should be involved in planning the curriculum for HSB, planning preventative actions and ensuring a whole-schools culture that condones HSB, alongside all other forms of abuse and harassment. This template policy provides a basis for an effective approach to managing sexual violence and harassment.

What is sexual violence?

The following are sexual offences under the [Sexual Offences Act 2003](#):

Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.

Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.

Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents. (NOTE- Schools and colleges should be aware that sexual assault covers a very wide range of behaviour so a single act of kissing someone without consent, or touching someone's bottom/breasts/genitalia without consent, can still constitute sexual assault.)

Causing someone to engage in sexual activity without consent: A person (A) commits an offence if: s/he intentionally causes another person (B) to engage in an activity, the activity is sexual, B does not consent to engaging in the activity, and A does not reasonably believe that B consents. (NOTE – this

could include forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.)

What is sexual harassment?

[Keeping Children Safe in Education Guidance 2022](#) and the [Sexual Violence and sexual harassment between children in schools and colleges](#) state:

When referring to sexual harassment we mean ‘unwanted conduct of a sexual nature’ that can occur online and offline and both inside and outside of school/college. When we reference sexual harassment, we do so in the context of child-on-child sexual harassment. Sexual harassment is likely to: violate a child’s dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names
- sexual “jokes” or taunting
- physical behaviour, such as: deliberately brushing against someone, interfering with someone’s clothes (schools and colleges should be considering when any of this crosses a line into sexual violence – it is important to talk to and consider the experience of the victim) and displaying pictures, photos or drawings of a sexual nature; and
- Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
- consensual and non-consensual sharing of nude and semi-nude images and/or videos. Taking and sharing nude photographs of U18s is a criminal offence.
 - sharing of unwanted explicit content
 - up skirting (this is a criminal offence)
 - sexualised online bullying.
 - unwanted sexual comments and messages, including, on social media.
 - sexual exploitation; coercion and threats.

It is important that schools and colleges consider sexual harassment in broad terms. Sexual harassment (as set out above) creates a culture that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

Responsibilities

Leaders and DSLs

Our leaders and DSLs have ultimate responsibility in dealing with all incidents of harmful sexual behaviour, including online. It is the expectation that all incidents of harmful sexual behaviour/sexual violence and harassment are reported in line with school safeguarding and child protection procedures.

We ensure that our designated safeguarding lead (DSL) and their deputy are confident in school safeguarding processes and when it is necessary to escalate. Our DSLs know what local and national specialist support is available to support all children involved in harmful sexual behaviour and are confident as to how to access this support when required.

Designated safeguarding lead/s and their deputies have an in-depth working knowledge of key documentation, particularly KCSIE 2022 and Sexual Violence and Sexual Harassment Between Children in Schools and Colleges (DfE 2021). We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

It is the role of school leaders and designated safeguarding leads to ensure that all staff and Governors receive training specific to harmful sexual behaviour, and that it is included as part of induction.

Staff

It is the responsibility of all staff to have read and understood this policy and associated policies. All staff must report any incidents or suspected incidents of harmful sexual behaviour to DSLs in line with school policy and ensure they are informed of the outcome. All staff will challenge any harmful sexual language or inappropriate behaviour. Staff have a duty to ensure that the school environment is one which is safe and which supports learners to understand safe and healthy relationships and appropriate behaviour through delivery of our curriculum.

Governors

We ensure that our governing body have a good understanding of what harmful sexual behaviour is, when it can pose a risk to children and how to keep children safe. Our governors receive regular training and updates, both in terms of what sexualised behaviour is, but also how to effectively support establishments and their stakeholders whilst holding provision to account.

As part of the headteacher's report, our governing body has the opportunity to monitor and evaluate the approach to harmful sexual behaviour to ensure it is adequate and effective. This includes evaluation of the curriculum, pupil voice activity and evaluation of parent/carers engagement. Governors ensure that risks relating to these issues are identified, that a number of reporting routes are available, and that risks are effectively mitigated.

Children

All children have the right to learn in a safe, healthy and respectful school environment. Our children benefit from an age-appropriate curriculum and are taught about healthy relationships and who they can go to for help. Our children know they will be believed if they make a disclosure and will be treated sensitively - whilst we cannot guarantee confidentiality, their thoughts and wishes will be taken into account when supporting them. Our staff understand that young children may not have the communication skills, and so are trained in recognising any changes in behaviour which may need further investigation from the DSL.

Parents/carers

We work hard to engage parents and carers by:

- sharing newsletters
- sharing information online e.g., website
- providing curriculum information

Our parents and carers are made aware of how and when to report any concerns to the school, that all incidents will be handled with care and sensitivity, and that it may sometimes be necessary to involve other agencies.

Vulnerable groups

We recognise that, nationally, vulnerable learners are three times more likely to be at risk from Harmful Sexual Behaviour. These include:

- A child with additional needs and disabilities.
- A child living with domestic abuse.
- A child who is at risk of/suffering significant harm.
- A child who is at risk of/or has been exploited or at risk of exploited (CRE, CSE),
- A care experienced child.
- A child who goes missing or is missing education.
- Children who identify as, or are perceived as, LGBTQI+ and/or any of the other protected characteristics.

Children displaying HSB have often experienced their own abuse and trauma. We ensure that any vulnerable learner is offered appropriate support, both within and outside school, sometimes via specialist agencies.

Reporting

All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via speaking with the DSL, reporting to the Police (101), NSPCC Helpline 0800 126 663, Children's Social Care (0300 123 6720) LADO (01772 536 694)

In this policy we recognise the importance of distinguishing between healthy, problematic and sexually harmful behaviour (HSB)

Our response is always based on sound safeguarding principles and follows school safeguarding processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

The school will always adopt a multi-agency approach and seek external support and guidance, in line with school policy, if deemed necessary. This may include:

Early Help, MASH, LADO, Police, Children's Social Care.

Training

The DSLs receive appropriate training delivered by LCC. Whole school training takes place annually, delivered by LCC Safeguarding Team.

Links

Child Exploitation and Online Protection command: [CEOP](#) is a law enforcement agency which aims to keep children and young people safe from sexual exploitation and abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors

The [NSPCC](#) provides a helpline for professionals at 0808 800 5000 and help@nspcc.org.uk. The helpline provides expert advice and support for school and college staff and will be especially useful for the designated safeguarding lead (and their deputies)

Support from specialist sexual violence sector organisations such as [Rape Crisis](#) or [The Survivors Trust](#)

The [Anti-Bullying Alliance](#) has developed guidance for schools about Sexual and sexist bullying.

The [UK Safer Internet Centre](#) provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues

[Internet Watch Foundation](#): If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)

[Childline/IWF Report Remove](#) is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online

[UKCIS Sharing nudes and semi-nudes advice](#): Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery).

[Thinkuknow](#) from NCA-CEOP provides support for the children's workforce, parents and carers on staying safe online

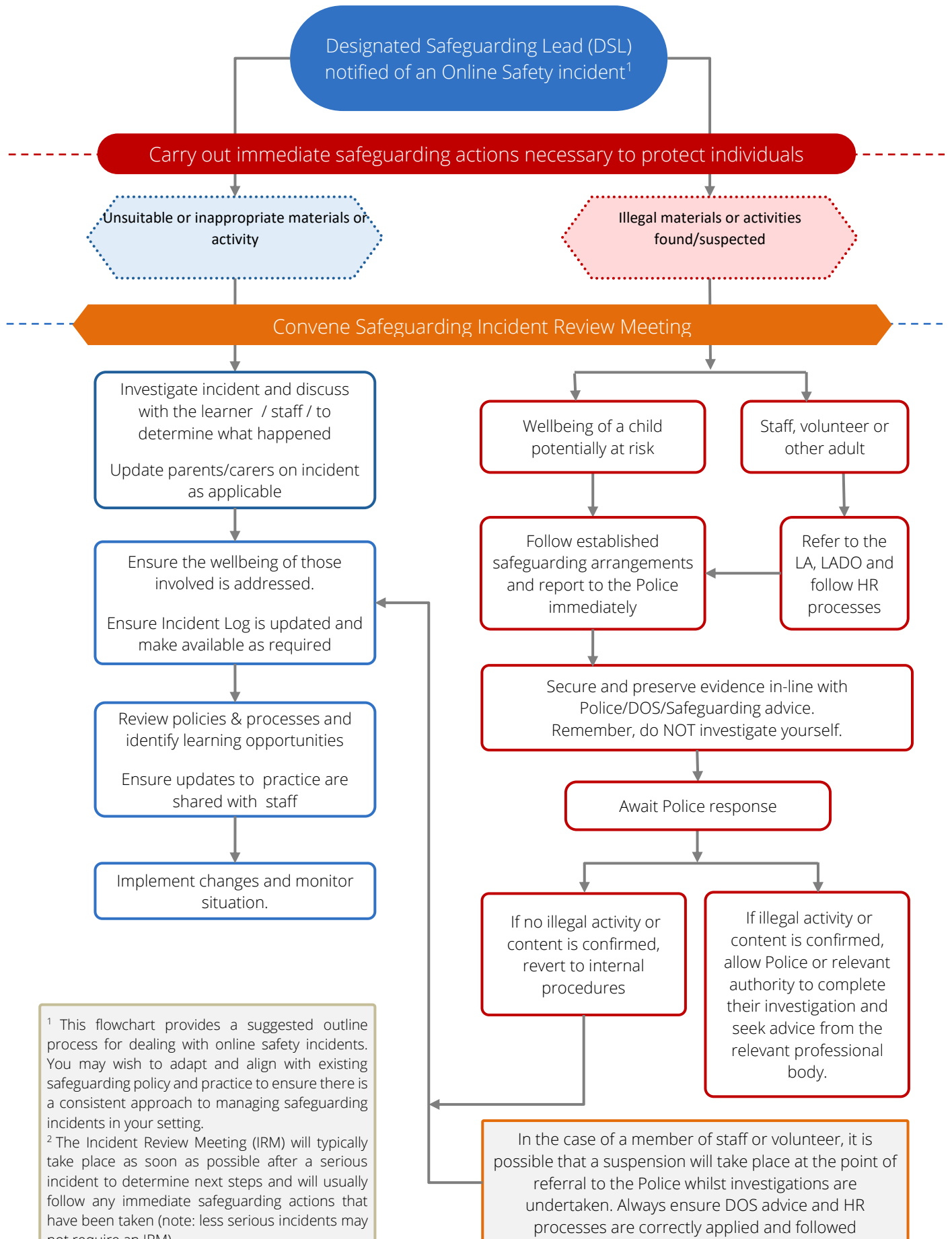
[Lucy Faithful Foundation](#)

[Marie Collins Foundation](#)

[NSPCC National Clinical and Assessment Service \(NCATS\)](#)

[Project deSHAME from Childnet](#) provides useful research, advice and resources regarding online sexual harassment.

Responding to incidents of misuse – flow chart 2025



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

Group:

Date:

Reason for investigation:

.....

.....

Details of first reviewing person

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

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

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Taywood Nursery School Reporting Log

Group:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Taywood Nursery School Training Needs Audit Log

Group:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

360safe.org.uk
360safe@swgfl.org.uk

