



The Children's House

Online Safety Policy

This policy should be reviewed annually and as required by legislation.		
Action	Reviewer	Date
Review	MZ / DF	Sep 2026
Approved by Chair of COM	AZ	Sep 2026
Date for next internal review		Sep 2027



The Children's House



Online safety is part of safeguarding. The Designated Safeguarding Lead (DSL) leads the School's safeguarding response to online concerns. Technical staff support this work but do not replace the DSL's safeguarding role.

Headteacher and Designated Safeguarding Lead (DSL); responsible SLT lead for filtering and monitoring	Ellie Grunewald elliegrunewald@childrenshouseschool.co.uk
Designated Safeguarding Lead and Early Years Safeguarding Co-ordinator	Mihaela Zama mihaelazama@childrenshouseschool.co.uk
Deputy Designated Safeguarding Lead; Deputy Headteacher; Looked After Children	Taiba Hussain taibahussain@childrenshouseschool.co.uk
Council of Management safeguarding link governor	Sarah Pitcher sarahpitcher@childrenshouseschool.co.uk
Council of Management online safety / digital link governor	Adam Zivanic adamzivanic@childrenshouseschool.co.uk
Head of Computing / Online Safety and Technical Lead	David Fonseca davidfonseca@childrenshouseschool.co.uk
School office	0207 354 2113

If you are worried about something online

A child may be at risk	Tell the DSL or a deputy DSL immediately. Do not wait for an IT check or investigation.
Sexual or intimate image	Tell the DSL immediately. Do not view, copy, print, save, forward or ask the child to send the image.
Concern about a member of staff	Report directly to the Headteacher. If the concern is about the Headteacher, report to the Chair of the Council of Management.
Filtering gap or technical problem	Tell the Head of Computing. If a child may have been exposed to harm, tell the DSL as well.
Data breach, phishing or cyber incident	Tell IT / the DPO route immediately. If pupil or safeguarding information may be affected, tell the DSL as well.
Immediate danger	Call 999 and follow the School's safeguarding procedures.



The Children's House

Key people and reporting contacts	2
Policy statement	3
1. Purpose and approach	4
2. Scope and related policies	4
3. Legal and guidance framework	4
4. Roles and responsibilities	5
5. Understanding online risks: the 4 Cs	6
6. Education and curriculum	6
7. Reporting and responding to concerns	7
8. Online bullying, child-on-child abuse and sexual imagery	8
9. Filtering and monitoring	8
10. Artificial intelligence and emerging technology	9
11. Data protection, cyber security and authorised systems	9
12. Mobile phones, personal devices and wearable technology	9
13. Images, video, social media and online communication	10
14. Remote learning and off-site use	11
15. Parents and carers	11
16. Training, review and governance	12
Appendix A - Online safety incident record	13
Appendix B - Key support and reporting contacts	15

Policy statement

The Children's House School wants children to benefit from technology while being protected from harm. Online safety is not a separate IT issue: it is part of safeguarding, behaviour, wellbeing, curriculum, data protection and the safe running of the School.

The School takes a whole-school approach. We combine age-appropriate education, clear behaviour expectations, safe systems, appropriate filtering and monitoring, staff training, parent partnership and prompt safeguarding action when concerns arise.

The best interests of the child come first. Where online activity raises a safeguarding concern, staff follow the School's Safeguarding and Child Protection Policy and report to the DSL without delay.



The Children's House

2

This policy explains how The Children's House School helps pupils use technology safely, responsibly and positively. It also explains what staff, governors, pupils, parents, visitors and contractors should do if an online concern arises. The policy is written for a primary school with Early Years provision. Our approach therefore takes account of children's age, development, individual needs and the fact that some pupils may be more vulnerable online, including pupils with SEND or additional communication, emotional or safeguarding needs.

The School recognises that online safety risks can arise on School devices, personal devices, websites, apps, games, social media, messaging services, artificial intelligence (AI), smart devices and through files shared directly between devices. Harm may begin outside school but still affect a pupil's safety, wellbeing or life in school.

We aim to help pupils become confident, curious and independent users of technology without expecting them to manage risks alone. Adults retain responsibility for appropriate supervision, teaching, safeguarding and professional judgement.

2

This policy applies to all members of the School community, including pupils, staff, governors, volunteers, contractors, visitors and parents/carers where they use School technology, services or communication channels, or where online behaviour affects the welfare of pupils or the School community.

It applies on both School sites, on trips and activities away from School, during remote or home learning, and when School accounts or devices are used away from the premises.

This policy should be read alongside the following School documents:

- Safeguarding and Child Protection Policy
- Behaviour Policy and Anti-Bullying Policy
- Staff Code of Conduct and Low-Level Concerns Policy
- ICT and Internet Acceptable Use Policy
- Mobile Phone and Electronic Device Use Policy
- Data Protection Policy and Information/Records Retention Policy
- Cyber Security Policy
- Artificial Intelligence Policy
- Camera and Image Policy
- PSHE / RSE Policy and Curriculum Policy
- Prevent risk assessment and safeguarding arrangements

Where there is any conflict between normal technology use and safeguarding a child, safeguarding takes priority. Data protection law does not prevent appropriate information sharing where this is necessary to protect a child; staff should seek advice from the DSL rather than delay a safeguarding response.

2

The School is an independent school in England and this policy has regard to current safeguarding, education, data protection and technology requirements. In particular, the School considers:

- [The Education \(Independent School Standards\) Regulations 2014](#) — statutory standards, including safeguarding and pupil welfare
- [Keeping Children Safe in Education 2026](#) — statutory safeguarding guidance
- [Working Together to Safeguard Children 2026](#) — statutory multi-agency safeguarding guidance
- [Early Years Foundation Stage statutory framework 2026](#) — statutory requirements for the School's Early Years provision
- [Relationships Education, RSE and Health Education guidance 2026](#) — statutory guidance
- [Mobile phones in schools](#) — statutory guidance from September 2026
- [Prevent duty guidance](#) — statutory guidance on the risk of radicalisation, including online
- [UK GDPR, Data Protection Act 2018 and Data \(Use and Access\) Act 2025](#) — data protection requirements
- [DfE Filtering and Monitoring Core Standard](#) — DfE recommended standard supporting safeguarding duties
- [Teaching online safety in schools](#) — DfE guidance for a whole-school curriculum approach



The Children's House

- [Generative AI in education and DfE AI product safety standards](#) — DfE guidance for safe and appropriate AI use
- The School will update its arrangements when statutory guidance or relevant national standards change. Operational details such as suppliers, filtering settings and technical configurations are held separately so that they can be changed without making this policy inaccurate.



Council of Management

- Ensure that safeguarding arrangements, including online safety, are effective and meet the Independent School Standards and current statutory guidance.
- Ensure appropriate filtering and monitoring is in place and receive assurance that its effectiveness is reviewed at least once each academic year.
- Provide strategic challenge and oversight, including through the safeguarding and online safety link governors, while recognising that safeguarding remains a collective responsibility of the Council of Management.
- Ensure governors receive safeguarding and child protection training, including online safety, appropriate to their role and kept up to date.

Headteacher and Designated Safeguarding Lead (DSL)

- Lead the School's safeguarding response to online safety concerns and ensure online safety is integrated into the wider safeguarding culture.
- Ensure staff know how to report online concerns and that concerns are assessed, recorded and referred to external agencies where required.
- Lead the School's annual review of filtering and monitoring as the responsible senior leader, with support from the DSL team and technical staff.
- Ensure online safety is reflected in staff training, curriculum planning, parent information, risk assessment and policy review.

Head of Computing / Online Safety and Technical Lead

- Support the DSL and senior leaders with technical knowledge about School systems, devices, filtering and monitoring.
- Carry out and record regular technical checks, review relevant monitoring information and promptly escalate safeguarding concerns to the DSL.
- Maintain appropriate technical documentation and help ensure that new systems, services and pupil-facing tools are considered for safeguarding, security, data protection and age suitability before use.
- Support staff training and curriculum development in online safety, AI, cyber security and responsible technology use.
- The technical role does not replace the DSL's responsibility for safeguarding decisions, referrals or case management.

All staff

- Read KCSIE Part One in full, follow the School's safeguarding procedures and complete required safeguarding training, including online safety and filtering and monitoring.
- Model safe, respectful and professional technology use and maintain appropriate boundaries online and offline.
- Supervise pupils appropriately, use School-approved systems and report concerns promptly, however small they may appear.
- Report filtering gaps, over-blocking, pupils bypassing protections, unsafe search results or other technical concerns so they can be reviewed.
- Never investigate a safeguarding concern themselves or promise confidentiality to a pupil.

Curriculum leads and teachers

- Provide age-appropriate and progressive online safety education across Computing, Relationships Education / PSHE and the wider curriculum.
- Adapt teaching for pupils who may need additional support, including pupils with SEND.



The Children's House

- Create opportunities for pupils to ask questions, practise critical thinking and learn how and where to seek help.

Data Protection Officer (DPO)

- Provide advice on personal data, privacy, data breaches and the use of new systems or AI where personal data may be processed.
- Work with the DSL and School leaders where a data incident also creates a safeguarding risk.

Pupils, parents, visitors and contractors

- Pupils are expected to follow their Acceptable Use Agreement, use School technology responsibly and tell a trusted adult if something worries, frightens or pressures them online.
- Parents/carers are encouraged to support the School's expectations, talk regularly with children about their online lives and raise concerns with the School promptly.
- Visitors, volunteers and contractors must follow School instructions and the relevant Acceptable Use, safeguarding, photography and device rules.



content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying,

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

KCSIE groups online safety risks into four broad areas. The School uses these "4 Cs" when planning teaching, reviewing incidents, considering new technology and reviewing filtering and monitoring.

Risks can overlap. For example, a pupil may receive harmful content, be contacted by an offender and then be pressured into harmful conduct. Staff should focus on the child's welfare and the full context rather than trying to fit an incident into only one category.

The School reviews its own incident patterns and pupil needs alongside national and local trends. Dated examples or particular apps are not treated as a complete list because platforms and risks change quickly.



Online safety is taught as part of a broad, balanced and age-appropriate curriculum. It is not limited to Computing lessons. The School uses opportunities across Computing, Relationships Education / PSHE, assemblies, class discussion, literacy and other subjects to build knowledge, confidence and healthy habits.

Teaching is planned so that pupils progressively learn to:

- **Recognise safe and unsafe situations:** know when something online is worrying, manipulative, sexual, violent, hateful, misleading or too good to be true.
- **Protect privacy and security:** understand personal information, passwords, location sharing, account security and the consequences of sharing information with others.
- **Build healthy relationships:** understand consent, respectful communication, boundaries, pressure, bullying, grooming and how online actions can affect other people.
- **Think critically:** check sources, recognise misinformation, fake accounts, manipulated media, advertising, influencer content and material created or altered with AI.



The Children's House

- **Understand permanence and reputation:** know that messages, images and recordings may be copied, forwarded or remain available after they appear to have been deleted.
- **Use technology positively:** develop creativity, communication, research and computing skills while understanding when to stop, ask for help or choose an offline activity.
- **Know how to report:** identify trusted adults and know how to report content, block contact and ask for help without fear of blame.

Teaching is adapted to the age and needs of pupils. Pupils with SEND or additional vulnerabilities may need more explicit teaching, repetition, visual support, individual guidance or additional supervision.

In the Early Years, technology use is purposeful and supervised. The School has regard to the EYFS framework on safe use of electronic devices and screen use, and balances digital experiences with conversation, play, movement, creativity and real-world interaction.

The School uses the principles of the UKCIS "Education for a Connected World" framework and DfE "Teaching online safety in schools" guidance to support progression. Curriculum content is reviewed annually and after significant incidents or changes in technology.



All online safety concerns are taken seriously. A concern does not need to have happened on a School device or on School premises for the School to respond if it may affect a child's safety, wellbeing or the School community.

What staff should do

- Listen calmly, take the child seriously and reassure them that they have done the right thing by speaking to an adult.
- Do not promise confidentiality. Explain that the information must be shared with people who can help keep them safe.
- Report the concern to the DSL or deputy DSL as soon as possible. Urgent safeguarding concerns must be reported immediately.
- Record what was seen, heard or reported using the School's safeguarding recording process, using the child's own words where possible and avoiding assumptions.
- Do not carry out your own investigation, contact alleged perpetrators, or ask a child to repeatedly explain what happened.
- Where a technical issue is involved, inform the Head of Computing after safeguarding has been secured, or at the same time where this can be done without delaying the DSL response.

Evidence

For ordinary online incidents, useful information may include usernames, web addresses, dates, times and a brief description. Staff should not create additional risk in order to collect evidence.

If the concern involves an intimate or sexual image of a child, staff must not intentionally view, copy, print, save, screenshot, forward or ask the child to send or download the image. Staff must not ask the child to delete it. The matter must be passed immediately to the DSL, who will follow current UKCIS guidance and safeguarding procedures.

Concerns about adults

Any concern or allegation about the online conduct of a member of staff, volunteer or contractor must be reported directly to the Headteacher in line with the Safeguarding and Child Protection Policy, Staff Code of Conduct and Low-Level Concerns Policy. If the concern is about the Headteacher, it must be reported to the Chair of the Council of Management. The LADO will be contacted where the criteria are met.

Recording and escalation

Safeguarding concerns are recorded within the School's safeguarding records. Technical incidents, security events and filtering/monitoring checks may also be recorded in the relevant IT or security log. Sensitive safeguarding details should not be duplicated unnecessarily in technical records.



The Children's House

The DSL decides, with appropriate advice, whether parents/carers, Children's Social Care, Police, CEOP, the LADO, Prevent partners or other agencies need to be involved. Parents/carers will normally be informed when their child is involved unless doing so may place a child at additional risk or affect an external safeguarding investigation.



Online behaviour can be a form of child-on-child abuse. The School applies the same safeguarding standards to behaviour that happens online as it does to behaviour in person. Harmful behaviour must not be dismissed as "banter", "just a joke" or part of growing up.

This includes online bullying and harassment, sexual harassment, coercion, threats, impersonation, fake profiles, discriminatory abuse, sharing private information, harmful group chats, grooming, image-based abuse and the creation or sharing of intimate images.

Intimate images, manipulated images and deepfakes

Any incident involving nude, semi-nude or sexually explicit imagery of a child is treated as a safeguarding concern. This includes images created or altered using AI, deepfake tools or other editing software, even where no original nude image existed.

Staff must follow the immediate reporting rules in section 7. The DSL will use current UKCIS guidance to decide the safest and most proportionate response, including whether external agencies or online removal services should be involved.

Coercion and financial extortion

If a child is being pressured to create or share sexual material, threatened that material will be shared, or asked for money, gaming credit or another benefit to prevent sharing, this must be treated as an urgent safeguarding concern. The child should be supported without blame or shame and the DSL should consider police / CEOP involvement.

Bullying outside school

Online bullying that begins outside school may still be addressed by the School where it affects pupils' safety, wellbeing, relationships or behaviour in school. Responses will follow the Safeguarding, Behaviour and Anti-Bullying policies and will consider support for all pupils involved as well as proportionate consequences.



Appropriate filtering and monitoring are part of the School's safeguarding arrangements. They support, but do not replace, good supervision, staff vigilance, a strong curriculum and children knowing how to ask for help.

The Council of Management ensures that appropriate filtering and monitoring systems are in place. The Headteacher leads the annual review of their effectiveness, supported by the DSL team and the Head of Computing. The review is recorded and completed at least once each academic year.

The School's arrangements are designed to:

- **Block harmful and inappropriate content:** while avoiding unreasonable disruption to legitimate teaching and learning.
- **Monitor appropriate indicators of risk:** so that safeguarding concerns can be identified and reviewed by suitable staff.
- **Cover the School's technology:** including internet-connected devices and locations used by pupils and staff, as appropriate to the risk.
- **Consider generative AI:** including access to AI services, AI-generated content and whether existing filtering and monitoring controls remain effective.
- **Keep clear records:** of annual reviews, regular checks, significant changes, identified gaps and actions taken.

The Head of Computing carries out regular operational checks and reviews relevant monitoring information. Any item that may indicate a safeguarding concern is passed to the DSL promptly. Technical staff should not make safeguarding decisions in isolation.



The Children's House

All staff have a role. Staff must report harmful material that is unexpectedly accessible, legitimate learning material that is unnecessarily blocked, attempts to bypass controls, use of unauthorised VPNs/proxies or personal hotspots by pupils, or any other concern about how filtering and monitoring is working.

Parents/carers are provided with clear information about the School's filtering and monitoring approach. The School recognises that no technical system can block every risk, particularly where pupils use personal devices or services outside the School network.



The School has a separate Artificial Intelligence Policy. This section explains how AI connects to online safety and safeguarding.

AI can support teaching and learning, but it can also produce convincing false information, harmful content, manipulated images and simulated conversations. KCSIE 2026 recognises that harmful contact may occur through generative AI applications that imitate human interaction and that AI-generated or manipulated sexual images may form part of online abuse.

At The Children's House School:

- **Approved and age-appropriate use:** pupil-facing AI tools must be approved by the School, suitable for the pupil's age and purpose, and appropriately supervised.
- **Safeguarding first:** harmful AI output, sexual content, grooming-like interaction, manipulation, threats or concerning AI conversations must be reported to the DSL.
- **Protect personal information:** staff and pupils must not place safeguarding records, medical information, SEND records, pupil photographs, contact details or other personal/sensitive information into unauthorised AI tools.
- **Human judgement remains essential:** AI must not replace professional decisions about safeguarding, behaviour, SEND, assessment or pupil welfare.
- **Filtering and monitoring applies:** the School considers the risks of generative AI when reviewing filtering, monitoring and new technology.
- **No harmful creation:** AI must not be used to create bullying, sexual, discriminatory, frightening, deceptive or impersonating content about pupils, staff or others.

New AI and digital tools are considered against DfE guidance and product safety standards, including age suitability, harmful content, privacy, security, manipulation, mental health, cognitive development and social or emotional development where relevant.



Online safety, data protection and cyber security overlap. Losing an account, exposing personal information or allowing unauthorised access can become a safeguarding issue when pupil information or key safeguarding systems are affected.

Staff must use School-approved systems for School work. Approved core systems include Microsoft 365 and iSAMS, together with other platforms authorised by the School. School information must not be moved to personal email accounts, personal cloud storage or unauthorised apps.

New platforms that process pupil information, allow communication, create pupil accounts or use AI must be approved before use. The School will consider safeguarding, privacy, data protection, security, age suitability, advertising/commercial features and how the service will be supervised and managed.

Use of School systems may be logged or reviewed where this is necessary and proportionate for safeguarding, security, compliance or investigation, in line with the School's Data Protection Policy and staff information.

Staff should be alert to phishing, impersonation, scams and unexpected requests for information or payment. Suspected cyber or data incidents must be reported promptly under the Cyber Security and Data Protection policies. If pupil or safeguarding information may be affected, the DSL must also be informed.

Information may be shared where necessary to safeguard a child. Staff should not allow uncertainty about data protection to delay a safeguarding referral; the DSL and DPO can advise on lawful and proportionate sharing.



The Children's House



The School is a mobile-phone-free environment for pupils during the School day, in line with the School's Pupil Use of Mobile Phones Policy and the DfE statutory guidance in force from September 2026. This expectation also applies to smart technology with similar communication, messaging or recording functions where the School has included it within its rules.

Pupils should not have access to a personal mobile phone during the School day. Any exception must be agreed in advance by the Headteacher for a clear reason, for example a medical, SEND, accessibility or other exceptional need, and appropriate safeguards will be put in place.

Staff, visitors, volunteers and contractors must follow the School's Mobile Phone and Electronic Device Use Policy. Personal devices must not be used to photograph, record or store pupil information unless specifically authorised under School procedure.

Smart glasses and wearable recording devices

Smart glasses, including Ray-Ban Meta glasses, and other wearable devices may capture photographs, video or audio, livestream, or send information to AI services. These rules apply to staff, pupils, parents/carers, visitors, volunteers and contractors on both School sites and during School trips and activities.

Anyone bringing such a device into School must tell reception or the member of staff welcoming them before entering areas used by children. The device must be switched off and put away unless the Headteacher has agreed an exception in advance. On trips, the person leading the visit must be informed.

These devices must not be used to photograph, film, record audio, livestream or send images or conversations to an AI service without prior authorisation from the Headteacher. Any authorised use must have a clear purpose and follow the School's safeguarding, data protection and Camera and Image Policy requirements. Permission to take photographs at a School event does not automatically permit recording through smart glasses or other wearable devices.

Where a device is needed for vision, a disability, a medical condition or accessibility, the School will discuss reasonable adjustments with the individual. Any agreed arrangement must protect privacy and prevent unauthorised recording or transmission.

If unauthorised recording is suspected, staff should ask the person to stop using the device and inform the Headteacher or DSL promptly. Staff must not attempt to search the device, copy recordings or require their deletion themselves. The Headteacher or DSL will coordinate the response, seeking data protection or police advice where appropriate. Any concern involving sexual or intimate imagery must be handled under section 7.

Staff must not provide unfiltered internet access through a personal hotspot or other personal connection. School devices and School-managed connections should be used for pupil learning unless an exception has been authorised.

On trips or activities away from School, communication arrangements are set through the trip risk assessment and School procedures. Any permitted use of a personal device for an emergency must protect staff privacy and pupil information.

Confiscation or examination of a device

Where a device is taken from a pupil under School policy, it should be stored securely and the relevant behaviour and safeguarding procedures followed. Staff should not routinely search through a pupil's device. Where content may raise a safeguarding concern, the Headteacher / DSL will decide the next steps in line with current law, guidance and School policy. The special rules in section 7 apply to sexual or intimate imagery.



Images, video and audio

Photographs and video of pupils must be taken, stored and shared in line with the Camera and Image Policy, Data Protection Policy and current parent/carer permissions or other appropriate lawful arrangements. School-approved devices and storage should be used.



The Children's House

Audio recordings and livestreams require the same care as photographs and video. Recording or transmitting lessons, meetings or conversations requires prior School authorisation and appropriate privacy arrangements. The additional rules for smart glasses and wearable recording devices are set out in section 12.

Pupil images or recordings must not be uploaded to unauthorised AI tools or personal services. Any manipulated, sexualised or harmful image of a pupil, including a deepfake, is a safeguarding concern and must be reported to the DSL.

Public-facing material should avoid unnecessary personal information. Staff must check the School's current permissions before publishing identifiable pupil images or video. Parents/carers attending School events should follow the School's instructions about photography and sharing images of other children.

School website and official social media

The School website and official social media accounts are managed by authorised staff. Content must protect pupils' privacy, respect copyright and present the School responsibly. Confidential pupil matters are not discussed through public or personal social media accounts.

Fake or impersonating accounts using the School's name, logo, staff identity or pupil identity should be reported to the School. Where there is a safeguarding risk, the DSL will lead the response; technical or platform reporting support may be provided by relevant staff.

Professional boundaries

Staff, governors, volunteers and contractors must maintain professional boundaries online. They must not use personal social media or private messaging to build personal relationships with pupils or communicate privately with pupils, except where a pre-existing family relationship has been declared and managed under School policy. Staff must not follow, friend or privately message pupil accounts. Pupils should not be encouraged to follow personal staff accounts. Staff should use privacy settings carefully but must understand that material shared privately may still become public.

The School does not encourage pupils to use social media or online services below the provider's stated minimum age. Online safety teaching nevertheless addresses the reality that some pupils may encounter these services outside School and focuses on safe behaviour and seeking help rather than blame.

Parents/carers should use the School's official communication and complaints routes rather than public social media when raising concerns about a child or the School.



The same safeguarding, behaviour, data protection and professional-boundary expectations apply when School technology is used away from School or when learning takes place remotely.

Staff should use School-approved accounts and platforms, consider what can be seen or heard during live communication, avoid unnecessary one-to-one private communication with pupils, and follow School arrangements for attendance, recording and parent/carer awareness.

Pupils using School devices at home remain subject to the Acceptable Use Agreement. The School will provide age-appropriate guidance to families about safe use, but parents/carers remain responsible for supervision and home internet arrangements outside School-managed services.



The School sees parents and carers as important partners in online safety. Families do not need to be technology experts; regular, calm conversations with children about what they do online are one of the most useful protective measures.

The School will:

- make this policy and related safeguarding information available to families
- provide clear information about filtering and monitoring and significant changes to School technology
- share practical guidance on online safety, mobile phones, AI, scams and emerging risks when appropriate
- listen to pupil and parent experiences when reviewing online safety provision
- contact parents/carers about incidents involving their child unless safeguarding reasons mean this would be unsafe or inappropriate at that time



The Children's House

Parents/carers are encouraged to respect age requirements for apps and services, use parental controls where appropriate, talk about online friends and contacts, support healthy sleep and screen habits, and tell the School promptly if an online issue is affecting their child or other pupils.



Staff and governor training

All staff receive safeguarding training at induction that includes online safety and an understanding of the School's filtering and monitoring arrangements. Safeguarding and online safety knowledge is updated at least annually and more often where risks, guidance or School systems change.

Governors receive safeguarding and child protection training, including online safety, so that they can provide effective strategic oversight and challenge.

Annual review and risk assessment

The School reviews this policy at least annually and sooner where there is a significant incident, a major change to technology, a change in statutory guidance or an identified gap in practice.

The annual online safety review considers the actual risks to pupils at The Children's House School, including age and developmental needs, SEND and vulnerability, incident records, pupil and staff feedback, filtering and monitoring information, local safeguarding context, use of AI and emerging technology, mobile devices and home/off-site use.

Filtering and monitoring effectiveness is formally reviewed at least once each academic year by the responsible senior leader, with support from the DSL and IT / technical support, and the outcome is recorded. Regular operational checks continue between formal reviews.

Relevant themes, incidents and assurance information are reported to the Council of Management through normal safeguarding and risk oversight arrangements. Reports should protect the confidentiality of individual pupils and staff.

The School will continue to use external guidance and self-review resources, including DfE standards, local safeguarding advice, UKCIS resources and 360safe / SWGfL materials, to support continuous improvement.



The Children's House



Safeguarding concerns should be recorded using the School's normal safeguarding recording process. This form may be used as a supporting record where needed. Do not attach or reproduce sexual images of children.

Name of person reporting	
Date and time reported	
Date / time of incident (if known)	
Where the incident happened	School / home / off-site / online / unknown

Child/children involved	
Other people involved	
Platform / service / device (if known)	
Safeguarding record reference	

Nature of concern (tick all that apply)

☐ Harmful / inappropriate content	☐ Online bullying / harassment
☐ Grooming / exploitation / coercion	☐ Intimate image / AI-generated or manipulated sexual image
☐ Impersonation / fake account	☐ Hate / discriminatory content
☐ Radicalisation / extremist content	☐ Self-harm / suicide content
☐ Scam / phishing / fraud / gambling	☐ Privacy / personal data concern
☐ Account misuse / hacking / bypassing safeguards	☐ Unauthorised or unsafe AI use
☐ Other	

What was reported / observed	Record facts and the child's own words where possible.
-------------------------------------	--



The Children's House

Immediate action taken	
Who was informed and when	DSL / Headteacher / IT / DPO / parent-carer / external agency as relevant
Outcome / follow-up	Support, referrals, platform action, filtering change, curriculum action, review date

Important: If the incident involves nude, semi-nude or sexually explicit imagery of a child, do not view, copy, screenshot, print, save, forward or ask the child to send/download/delete the image. Report to the DSL immediately.



The Children's House



Internal reporting should always follow the School's safeguarding procedures first. The DSL will decide when external reporting or specialist support is required.

Service	Contact	Use
Emergency services	999	Immediate danger or emergency
Islington Children's Social Care	020 7527 7400 / CSCTReferrals@islington.gov.uk	Safeguarding referrals and advice
Islington LADO	LADO@islington.gov.uk	Allegations about adults working with children; normally contacted by the Headteacher/DSL
CEOP Safety Centre	https://www.ceop.police.uk/Safety-Centre/	Online sexual abuse, grooming and exploitation
Internet Watch Foundation (IWF)	https://www.iwf.org.uk/	Reporting child sexual abuse material online
Report Remove / Childline	https://www.childline.org.uk/remove	Support for under-18s to report and remove nude or sexual images shared online
Professionals Online Safety Helpline	https://saferinternet.org.uk/professionals-online-safety-helpline	Specialist advice for professionals
Report Fraud	https://www.reportfraud.police.uk/	National reporting route for fraud and cyber crime in England, Wales and Northern Ireland

Key national guidance used for this policy

- [The Education \(Independent School Standards\) Regulations 2014](#)
- [Keeping Children Safe in Education 2026](#)
- [Working Together to Safeguard Children 2026](#)
- [Early Years Foundation Stage statutory framework 2026](#)
- [Relationships Education, RSE and Health Education guidance 2026](#)
- [Mobile phones in schools](#)
- [Prevent duty guidance](#)
- [UK GDPR, Data Protection Act 2018 and Data \(Use and Access\) Act 2025](#)
- [DfE Filtering and Monitoring Core Standard](#)
- [Teaching online safety in schools](#)
- [Generative AI in education and DfE AI product safety standards](#)

This policy was prepared for The Children's House School and should be read alongside the School's current Safeguarding and Child Protection Policy and local safeguarding procedures.