The Children’s House

Online Safety Policy

This policy should be reviewed annually and as required by legislation.		
Action	**Reviewer**	**Date**
Review	EG/MZ	September 2025
Approved by Chair of COM	BB/ AZ	September 2025
Date for next internal review		July 2026

The Children's House

Introduction

Key people / dates

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Ellie Grunewald elliegrunewald@childrenshouseschool.co.uk Telephone number (term time): 0207 354 2113 (option 1) Mobile number: 07961 451 226
Designated Safeguarding Lead and Coordinator (Nursery)	Mihaela Zama mihaelazama@childrenshouseschool.co.uk Telephone number (term time): 0207 354 2113 (option 1) Mobile number: 07882 732 612
Deputy Designated Safeguarding Lead	Taiba Hussain taibahussain@childrenshouseschool.co.uk Telephone number (term time): 0207 354 2113 (option 2) Mobile number: 07759398972
Deputy Designated Safeguarding Lead	Laura Mills Lauramills@childrenshouseschool.co.uk Telephone number (term time): 0207 354 2113 (option 1)
Deputy Designated Safeguarding Lead	Kim Crawford Kimcrawford@childrenshouseschool.co.uk Telephone number (term time): 0207 354 2113
Link governor for safeguarding	Sarah Pitcher Sarahpitcher@childrenshouseschool.co.uk
Link governor for Online Safety	Adam Zivanic adamzivanic@childrenshouseschool.co.uk
Online Safety, Digital Learning & Technical Support Lead	Email: davidfonseca@childrenshouseschool.co.uk Telephone number (term time): 0207 354 2113 (option 1) Mobile number: 07516937163

The Children's House

What is this policy?

This policy serves as our comprehensive approach to online safety within The Children's House School. It aligns with key statutory documents, including 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE (Relationships, Sex and Health Education) guidance, and other relevant statutory documents.

Our online safety policy is designed to be cross-curricular, extending its relevance beyond subjects such as Relationships, Health and Sex Education, Citizenship and Computing. It is intended to complement our school's statutory Child Protection and Safeguarding Policy.

All matters and concerns related to online safety are subject to our school's safeguarding and child protection procedures. This policy outlines our commitment to fostering a safe online environment for The Children's House School community, ensuring that the well-being of our students is a top priority.

Who is it for? When is it reviewed?

This policy is intended for all members of The Children's House School community, including staff, governors, pupils and parents. It is a living document, subject to a comprehensive annual review and amendments throughout the year, as needed, in response to changes within the school and the local area.

While many aspects of this policy are informed by legislation and regulations, we place great importance on involving all stakeholders in its creation and review. This collaborative approach ensures that the policy is clear, practical, and can be followed effectively in all respects. It also helps in fostering a deep understanding among stakeholders regarding the rules in place and their rationale, thus impacting day-to-day practices.

Who is in charge of online safety?

At The Children's House School, online safety is overseen by the Designated Safeguarding Lead (DSL). KCSIE (Keeping Children Safe in Education) specifies that the DSL holds the primary responsibility for safeguarding and child protection, including online safety. While the DSL can delegate specific activities related to online safety, the ultimate responsibility for this area remains with the DSL.

Subject leads, such as those responsible for Relationships, Sex and Health Education (RSHE) and teachers collaborate to plan the curriculum for their respective areas. It is crucial that these curriculum plans align with the school's whole-school approach to online safety, ensuring a cohesive and comprehensive strategy. At the Children’s House, RSHE is currently overseen by the Headteacher.

What are the main online safety risks

Current Online Safeguarding Trends

Over the past year, we have observed various trends related to device use, online activities and incidents that impact the safety and well-being of our students. These trends provide valuable insights, shaping the online safety policies and practices within The Children’s House School community.

In developing our policies and acceptable use agreements, we consider both specific trends within our school community and the broader online safeguarding trends nationally.

We adhere to the guidelines outlined in KCSIE (Keeping Children Safe in Education), which groups online safety risks into four areas, known as the "4 Cs":

1. **Content** (Illegal, Inappropriate/harmful eg: fake news, racism, misogyny, self-harm, extremism, pornography, misinformation, disinformation and conspiracy theories; content validation: how to check authenticity and accuracy of online content)
2. **Contact** (online bullying in all forms, grooming, sexual harassment, sexual exploitation, radicalisation, influencing)
3. **Conduct** (privacy, digital footprint, health and wellbeing, nudes and semi-nudes, sexting, copyright, live streaming)
4. **Commerce** (online gambling, advertising, phishing scams, financial scams, micro-transactions)

We acknowledge that these trends are continually evolving, and we remain committed to adapting our policies as needed, especially in response to any potential changes resulting from the Online Safety Bill becoming law.
Some noteworthy national trends and issues over the past year include:

- **Self-generative Artificial Intelligence:** Students now have access to tools that can generate text and images. These tools pose challenges in terms of accuracy when students seek information. Moreover, they raise concerns about plagiarism for teachers and safety issues since many of these tools lack end-user safety settings, age restrictions, and can produce inappropriate content. It is essential to address this, not only within the school environment, but also by educating students and parents about the responsible use of these tools at home.
- **Increased Online Time:** The continued cost-of-living crisis has led children to spend more time online, exposing themselves to various online harms. Families have reduced leisure activities, and public provisions for free youth activities have decreased. This increased online exposure necessitates a focus on online safety education.
- **Usage of Popular Apps:** The Ofcom report highlights that YouTube remains the most used site or app among all under-18s, with the reach of apps like WhatsApp, TikTok and Snapchat increasing. Many students are on these apps regardless of age limits, which are often misunderstood or ignored. Addressing best practices while understanding the reality of students' app usage is essential.
- **Early Mobile Phone Access:** A significant number of young children have access to mobile phones, with a lack of safety controls or restrictions. Children as young as 3 to 6 have been exposed to 'self-generated' sexual content, and there has been a disturbing rise in cases of child sexual abuse material within the 7-10 age group.
- **Influence of Misogynistic Content:** The rise of misogynistic influencers, such as Andrew Tate, has significantly influenced many young boys. This influence has challenged schools to address inappropriate behaviours.
- **Social Media as a Source of News:** More children and young people are using apps like Snapchat as their primary source of news and information, often without attention to the credibility of influencers sharing news. This content is frequently interspersed with disturbing and illegal content.
- **Filming and Sharing of Fights:** Schools have seen an increase in issues related to fights being filmed and shared, which is a concerning trend.
- **Exposure to Harmful Content:** An increasing number of students are exposed to content promoting self-harm and sexual abuse coerced with threats of violence, including cases in primary schools.
- **Fake Profiles:** There is a rise in fake profiles causing problems for schools, where the school's logo and name are used to share inappropriate content about students and defamatory allegations about staff. These profiles are also used for bullying and impersonation.

We are committed to addressing these trends and issues within The Children's House School specific context and ensuring that our policies and practices provide a safe and secure online environment for our younger students, all within the framework of the 4 Cs for a comprehensive approach to online safety.

How will this policy be communicated?

This policy will be communicated through various channels to ensure accessibility and understanding by all stakeholders in The Children's House School community. The communication methods include:

- **Posting on the School Website:** The policy will be readily accessible to all on our school's website.

- **Inclusion in School Induction Pack:** All new staff, including temporary, supply and non-classroom-based staff, as well as those starting mid-year, will receive this policy as part of their induction pack.
- **Integral to Safeguarding Updates and Training:** The policy will be integrated into our safeguarding updates and training sessions for all staff. Special emphasis on this policy will be given during refreshers, especially at the beginning of the academic year.
- **Acceptable Use Policies (AUPs):** The principles outlined in this policy will be clearly reflected in the AUPs for staff, volunteers, contractors, governors, pupils, and parents/carers. These AUPs will be issued to the whole school community on entry to the school, annually, and whenever changes are made.

The Children's House

Contents

Overview

Aims

This online safety policy at The Children's House School is designed to promote a holistic approach to online safety by:

- Defining the expectations for all members of The Children's House School community regarding their online behaviour, attitudes, and digital technology usage, including when devices are offline.
- Enhancing the understanding and awareness of online safeguarding aspects among safeguarding and senior leadership teams through effective collaboration and communication with technical staff, curriculum leads (e.g., RSHE), and other relevant stakeholders.
- Emphasizing that standards of online and digital behaviour, including social media activity, must be upheld beyond the school premises and operating hours. These standards apply consistently, irrespective of the device or platform used.
- Promoting the safe, responsible, respectful, and positive utilization of technology to support teaching and learning, enhance academic achievement, and prepare children and young individuals to navigate the challenges and opportunities of today's and tomorrow's digital world. Our goal is for them to not only survive but thrive online.
- Ensuring that school staff working with children comprehend their roles and responsibilities for safe and responsible use of technology and the online environment. This includes protection and support for the children under their care, their own safety and reputation, and upholding the school's ethos and objectives.
- Establishing clear protocols for addressing online misconduct and providing guidance on procedures to follow when there are doubts or concerns, with references to other school policies like the Behaviour Policy or Anti-Bullying Policy.

By outlining these aims and expectations, The Children's House School endeavours to create a safe, respectful, and constructive online environment for all members of our community.

Further Help and Support

At the Children's House School, we prioritise internal school channels for reporting and support, in line with our school policy documents, especially when addressing incidents. All incidents should be reported in accordance with our Child Protection & Safeguarding Policy. The Designated Safeguarding Lead (DSL) is responsible for handling referrals to local authority multi-agency safeguarding hubs (MASH), and typically, the headteacher, also the DSL, will manage referrals to the Local Authority Designated Officer (LADO). Additionally, the local authority, academy trust, or any third-party support organizations we collaborate with may have advisors available to provide general support.

However, for additional external support and resources, we recommend the following:

- reporting.lgfl.net: This resource provides a curated list of external support and helplines, accessible to both pupils and staff. These include:
  - **Professionals' Online-Safety Helpline** from the UK Safer Internet Centre.
  - **NSPCC Report Abuse Helpline** for reporting incidents of sexual harassment or abuse.
  - Helplines for reporting hate crimes, terrorist activities, and fraud, which may be valuable to share with parents.
  - Anonymous support resources for children and young people.
- **Training**: For those seeking training on online safety, resources are available via safetraining.lgfl.net.

We are committed to providing our school community with the necessary resources and support to ensure online safety.

Scope

This policy applies to all members of The Children's House School community, including teaching, supply, and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors, and community users. It encompasses individuals who have access to our digital technology, networks and systems, whether on-site or remotely and at any time, as well as those who use technology in their roles within our school.

Roles and Responsibilities

The Children's House School is a community, and all its members share a collective responsibility to exhibit respectful behaviour both online and offline. We recognize the value of technology in teaching, learning and preparing for life beyond school. It is imperative that every member of our community promptly reports any concerns or inappropriate behaviour. This is essential to safeguard our staff, pupils and community. Each member of our school community should familiarise themselves with the relevant section in Annex A of this document, which outlines individual roles and responsibilities. It is crucial to note that there is a section titled "All Staff," which must be read by every staff member, even if they have specific responsibilities described in another section. The annex also contains role descriptions for pupils, governors and other relevant roles.

In the academic year 2025/2026, it is paramount that all members of our community understand their responsibilities concerning filtering and monitoring. All staff members play a crucial role in providing feedback on potential issues. This collaborative effort is essential for maintaining a safe and secure online environment.

Education and curriculum

It is of paramount importance for schools to establish a well-structured curriculum for online safety that progresses in a manner relevant to the pupils' developmental stages. This curriculum should not only provide pupils with the fundamental knowledge and behaviours to navigate the online world safely but also equip them to confidently use digital technology across various devices, platforms and applications.

Teaching Online Safety in Schools advocates for the integration of online safety and understanding of potential harms through a whole-school approach. This approach enables tailoring teaching and offers support to address the specific needs of pupils, including those who may be more vulnerable. To facilitate this, dedicated training is available with curriculum mapping for Relationship, Sex and Health Education (RSHE) / Personal, Social, Health and Economic Education (PSHE) and Online Safety Lead s. Further information can be accessed at safetraining.lgfl.net.

The RSHE guidance recommends assessing teaching to identify where pupils may require extra support or intervention. LGfL provides the SafeSkills Online Safety Quiz and diagnostic teaching tool linked to statements from the UKCIS Education for a Connected World framework. These tools allow teachers to monitor progress and to identify areas for development. Access to these resources can be found at safeskillsinfo.lgfl.net.

The following subjects have the most direct connections to online safety:

- Relationships education, relationships and sex education (RSE) and health (RSHE/PSHE)
- Computing
- Citizenship

However, as outlined in the role descriptors above, it is the responsibility of all staff to identify opportunities to integrate online safety into all school activities, within and outside the curriculum. Staff should also be prepared to leverage unexpected learning opportunities as they arise, as these can offer unique value to pupils.

Whenever technology is used within the school, whether for classroom activities or homework assignments, all staff should promote sensible use, monitor pupils' activities, consider potential risks, and assess the age appropriateness of websites. Furthermore, it's essential to provide clear information to parents and carers about what systems the school uses for filtering and monitoring online use. They should also understand the activities their children are engaging in and with whom they are interacting online.

Likewise, all staff members should offer guidance and supervision when pupils are involved in online learning activities, extra-curricular activities, extended school programs, remote teaching or other online endeavours. This includes support for search skills, critical thinking (e.g., evaluating disinformation, misinformation and fake news), ensuring age-appropriate materials, addressing legal issues such as copyright and data laws, and providing information and signposting. Teachers and parents can access regularly updated theme-based resources, materials and signposting at saferesources.lgfl.net.

At The Children's House School, we acknowledge that online safety and digital resilience should be integrated throughout the curriculum. To achieve this, we are working to implement the cross-curricular framework 'Education for a Connected World – 2020 edition' from the UK Council for Internet Safety (UKCIS). This framework encompasses graduated statements for different age groups: EYFS-7, 7-11, 11-14, and 14-18.

We conduct annual reviews of curriculum plans and schemes of work, including adaptations for pupils with special educational needs and disabilities (SEND). These reviews are an opportunity to closely align the curriculum with the UKCIS framework's key areas, which cover Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security and Copyright and ownership.

For further details on our curriculum and progression model, please visit the link to curriculum. These curriculum reviews are conducted in the context of an annual online safety audit, which is a collaborative effort between the DSL and IT Coordinator/Technician.

Handling Safeguarding Concerns and Incidents

Online safety is a vital component of safeguarding, in addition to being a fundamental aspect of Computing, PSHE/RSHE and Citizenship within the curriculum. General concerns related to online safety must be handled in the same way as any other safeguarding concern. Safeguarding is often compared to a jigsaw puzzle and all stakeholders should prioritize communication with the Online Safety Lead or Designated Safeguarding Lead to contribute to the overall picture or bring attention to potential issues that might not have escalated to a problem yet.

Support staff often have a unique perspective and the opportunity to identify issues first in areas outside the classroom, such as the playground, toilets, and other communal spaces. This is particularly relevant to concerns related to bullying, sexual harassment and violence.

School procedures for addressing online safety matters are primarily outlined in the following policies.

- Safeguarding and Child Protection Policy
- Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy
- Cybersecurity Policy

The Children's House School is committed to taking all reasonable precautions to safeguard pupils online. However, we acknowledge that incidents can occur both inside and outside of school, with potential impacts when students enter school or during extended periods away from school. All members of the school community are encouraged to report issues promptly to allow us to address them swiftly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the Online Safety Lead or Designated Safeguarding Lead on the same day. In urgent cases, reports will be made by the end of the lesson.

Concerns or allegations regarding staff misuse are always referred directly to the Headteacher. In cases where the concern pertains to the Headteacher, the complaint is referred to the Chair of Governors and the Local Authority's Designated Officer (LADO). Staff members may also use the NSPCC Whistleblowing Helpline, and posters with relevant contact details are displayed in the staff room.

The school will actively seek support from external agencies when necessary, including the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, Internet Watch Foundation (IWF), and the Harmful Sexual Behaviour Support Service.

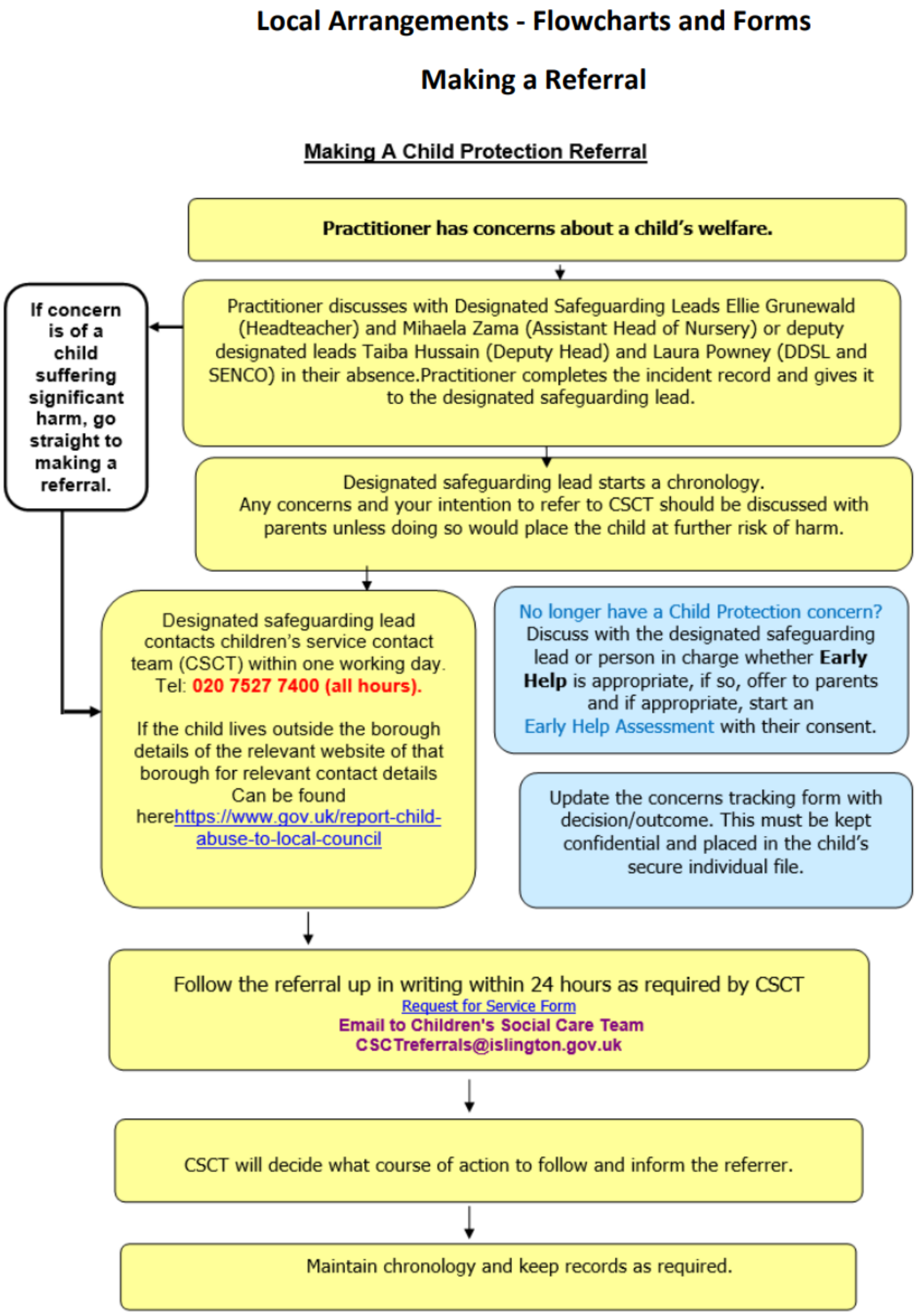
The Department for Education's guidance "Behaviour in Schools, advice for headteachers and school staff" (February 2024) provides advice and outlines related legal duties, including support for pupils and the authority of staff when addressing incidents. Parents and carers will be informed of online safety incidents involving their children. Additionally, the Police will be contacted when staff or pupils engage in behaviour that is particularly concerning or breaks the law. Specific procedures are in place for sexting and upskirting.

The school will evaluate whether reporting procedures are suitable for potential future closures, lockdowns, periods of isolation, etc., and will make alternative provisions in advance when necessary.

The Children's House

Actions where there are concerns about a child.

As outlined previously, online safety concerns are no different to any other safeguarding concern. See below the flowchart for making a referral



Local Arrangements - Flowcharts and Forms

Making a Referral

Making A Child Protection Referral

Practitioner has concerns about a child's welfare.

Practitioner discusses with Designated Safeguarding Leads Ellie Grunewald (Headteacher) and Mihaela Zama (Assistant Head of Nursery) or deputy designated leads Taiba Hussain (Deputy Head) and Laura Powney (DDSL and SENCO) in their absence.Practitioner completes the incident record and gives it to the designated safeguarding lead.

If concern is of a child suffering significant harm, go straight to making a referral.

Designated safeguarding lead starts a chronology.
Any concerns and your intention to refer to CSCT should be discussed with parents unless doing so would place the child at further risk of harm.

Designated safeguarding lead contacts children's service contact team (CSCT) within one working day. Tel: **020 7527 7400 (all hours).**

If the child lives outside the borough details of the relevant website of that borough for relevant contact details Can be found herehttps://www.gov.uk/report-child-abuse-to-local-council

No longer have a Child Protection concern? Discuss with the designated safeguarding lead or person in charge whether **Early Help** is appropriate, if so, offer to parents and if appropriate, start an Early Help Assessment with their consent.

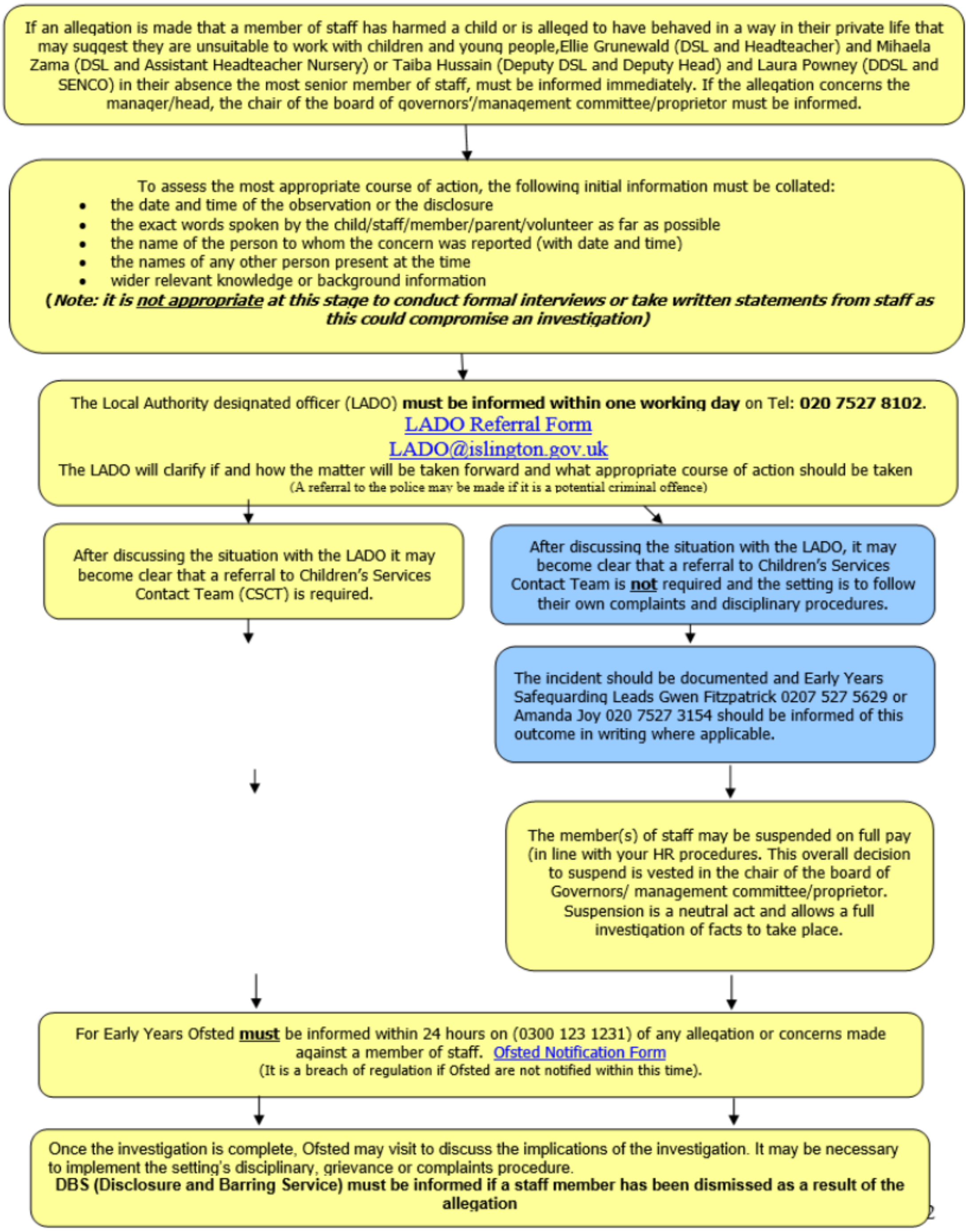
Update the concerns tracking form with decision/outcome. This must be kept confidential and placed in the child's secure individual file.

Follow the referral up in writing within 24 hours as required by CSCT
Request for Service Form
Email to Children's Social Care Team
CSCTreferrals@islington.gov.uk

CSCT will decide what course of action to follow and inform the referrer.

Maintain chronology and keep records as required.

The Children's House



If an allegation is made that a member of staff has harmed a child or is alleged to have behaved in a way in their private life that may suggest they are unsuitable to work with children and young people,Ellie Grunewald (DSL and Headteacher) and Mihaela Zama (DSL and Assistant Headteacher Nursery) or Taiba Hussain (Deputy DSL and Deputy Head) and Laura Powney (DDSL and SENCO) in their absence the most senior member of staff, must be informed immediately. If the allegation concerns the manager/head, the chair of the board of governors'/management committee/proprietor must be informed.

To assess the most appropriate course of action, the following initial information must be collated:

- the date and time of the observation or the disclosure
- the exact words spoken by the child/staff/member/parent/volunteer as far as possible
- the name of the person to whom the concern was reported (with date and time)
- the names of any other person present at the time
- wider relevant knowledge or background information

(Note: it is not appropriate at this stage to conduct formal interviews or take written statements from staff as this could compromise an investigation)

The Local Authority designated officer (LADO) **must be informed within one working day** on Tel: **020 7527 8102.**

LADO Referral Form

LADO@islington.gov.uk

The LADO will clarify if and how the matter will be taken forward and what appropriate course of action should be taken

(A referral to the police may be made if it is a potential criminal offence)

After discussing the situation with the LADO it may become clear that a referral to Children's Services Contact Team (CSCT) is required.

After discussing the situation with the LADO, it may become clear that a referral to Children's Services Contact Team is **not** required and the setting is to follow their own complaints and disciplinary procedures.

The incident should be documented and Early Years Safeguarding Leads Gwen Fitzpatrick 0207 527 5629 or Amanda Joy 020 7527 3154 should be informed of this outcome in writing where applicable.

The member(s) of staff may be suspended on full pay (in line with your HR procedures. This overall decision to suspend is vested in the chair of the board of Governors/ management committee/proprietor. Suspension is a neutral act and allows a full investigation of facts to take place.

For Early Years Ofsted **must** be informed within 24 hours on (0300 123 1231) of any allegation or concerns made against a member of staff. Ofsted Notification Form

(It is a breach of regulation if Ofsted are not notified within this time).

Once the investigation is complete, Ofsted may visit to discuss the implications of the investigation. It may be necessary to implement the setting's disciplinary, grievance or complaints procedure.

DBS (Disclosure and Barring Service) must be informed if a staff member has been dismissed as a result of the allegation

Islington Referral form (please use link)

https://www.islingtoncs.org/sites/default/files/files/Request%20for%20Service%20Form%202020.docx

Bullying

Online bullying, including incidents that occur outside of school or from home, should be addressed following the same procedures as any other form of bullying. The school's bullying policy found here should be applied to online bullying, also referred to as cyberbullying, including incidents that result from banter.

It is important to note that over the past 12 months, there has been an increase in anecdotal reports of fights being filmed and fake profiles being used to bully children on behalf of others. Staff will be reminded of these specific issues when addressing bullying.

Materials to support teaching about bullying, as well as useful guidance and case studies provided by the Department for Education, are available here.

Misuse of School Technology (devices, systems, networks or platforms)

Clear and well-communicated rules and procedures are essential to govern the use of The Children's House School networks, connections, internet connectivity, devices, cloud platforms and social media by both students and adults. These rules and procedures are defined in the Acceptable Use Policy, with sections that pertain to staff, pupils and parents. This policy covers aspects such as professional and personal use of school platforms, networks, clouds, devices and other technology.

When students violate these rules, the school's Behaviour Policy will be applied. If staff members contravene these rules, action will be taken in accordance with the Staff Code of Conduct. It's essential to reinforce these rules at the beginning of each school year and to remind students that the same applies to any home learning that may occur during periods of absence, closure, quarantine or similar situations.

In addition to these steps, the school reserves the right to temporarily or permanently withdraw access to such technology or the right to bring personal devices onto school property.

With the new responsibilities for filtering and monitoring, led by the DSL and following the new DfE standards, it is possible that more such incidents will be discovered. The Children's House School will make efforts to remind both students and staff of this increased scrutiny at the start of the school year.

Data Protection and Cybersecurity

The Children's House School takes data protection and cybersecurity seriously. All pupils, staff, governors, volunteers, contractors and parents are expected to adhere to our Data protection and Cybersecurity policy, which can be found here. It's essential to recognize that the proper handling of data and cybersecurity practices is closely tied to our ability to safeguard children effectively.

This commitment aligns with the guidance provided in KCSIE and references the DfE Cybersecurity standards. It is crucial to understand that data protection regulations do not hinder the sharing of information when it is essential for the safety and welfare of children. As highlighted in *Data protection in Schools 2023*, there's generally no need to seek consent to share personal information for safeguarding purposes. KCSIE emphasizes that the Data Protection Act 2018 and UK GDPR support the sharing of information when it is necessary to safeguard and promote the welfare and safety of children. We encourage open communication and collaboration within our school community to ensure the safety and protection of all our students.

Appropriate Filtering and Monitoring

At The Children's House School, we take online safety seriously and understand the importance of appropriate web filtering and monitoring to protect our students while ensuring that learning can proceed effectively. This approach aligns with the requirements of Keeping Children Safe in Education (KCSIE) and the DfE filtering and monitoring standards. We also use DfE's 'plan technology for your school' service.

The Designated Safeguarding Lead (DSL), Ellie Grunewald, holds the primary responsibility for filtering and monitoring within our school, supported by the named governor responsible for these areas.

In line with the DfE standards, we have established the following measures:

- Roles and responsibilities have been identified and assigned for managing filtering and monitoring systems.
- We conduct an annual review of our filtering and monitoring provision.
- Our systems are configured to block harmful and inappropriate content without unreasonably disrupting teaching and learning.
- Effective monitoring strategies are in place to meet our safeguarding requirements.

To achieve the best outcomes in these areas, we encourage close collaboration between our technical teams and safeguarding teams. Regular checks are conducted to ensure our systems are functioning correctly and to identify areas of concern. All staff play a vital role in providing feedback, reporting concerns and addressing potential issues related to filtering and monitoring.

Our staff receive reminders about the systems in place and their responsibilities during induction, at the start of the school year and through our Acceptable Use Policies (AUPs). We also provide training to ensure that all staff members are well-informed and equipped to contribute to the safety of our students.

Understanding the nuances of filtering, monitoring, over blocking and related terms is essential. We provide guidance videos, written information and training to support our staff in this regard.

At The Children's House School:

- Web filtering is provided by Aerial Direct, school premises.
- The DSL holds overall responsibility for filtering and monitoring.
- Technical support and advice, setup and configuration are provided by the Head of IT.
- Regular checks are carried out on a half-termly basis by the Head of IT to ensure filtering is consistently effective and functional across all areas.

- An annual review is conducted as part of the Online Safety Audit ensuring a comprehensive approach to online safety. [

The DfE standards suggest a range of monitoring strategies to minimise safeguarding risks. At our school, we use Watchguard Content Filtering. This approach ensures the safety and security of our students while they access online resources.

Artificial Intelligence (AI)

The Children's House recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. Bullying and grooming) and/or expose pupils to harmful content, for example, in the form of 'Deepfakes', where AI is used to create images, audio or video hoaxes that look real. Any AI tool used by the school should first be risk assessed.

The Children's House school will treat any use of AI to access harmful content or bully pupils in line with this policy and our anti-bullying and behaviour policies.

The Department has published Generative AI: product safety expectations - GOV.UK and explains how filtering and monitoring requirements apply to the use of generative AI in education.

Authorised Systems

At The Children's House School, we prioritize the use of authorised systems for all communications involving staff, students, and parents. We adhere to the following guidelines to maintain the privacy and security of all stakeholders and ensure compliance with safeguarding best practices and UK data protection legislation:

1. **Email System**: Staff members use the email system provided by Microsoft for all school-related emails. These accounts are administered by the school and are not linked to personal/private email accounts.
2. **School Administration System**: ISAMS is utilised for all school-related data management, including student information. This system is centrally managed and administered by the school, ensuring it can be monitored and audited centrally.
3. **Messaging Platforms**: Staff never use personal/private email accounts or other messaging platforms to communicate with children, parents or colleagues when discussing school or child data. All communication must take place through school-administered systems to maintain a secure and safeguarded environment.
4. **Central Management**: All systems used for school-related communication are centrally managed to protect children against abuse, safeguard staff members from potential allegations, and comply with UK data protection legislation.
5. **Approval for New Platforms**: Any introduction of a new platform with communication facilities or any system requiring child logins, or the storage of school/child data must be approved in advance by the school and centrally managed. This procedure ensures that the platform aligns with our safeguarding and data protection standards.
6. **Unauthorised Use**: Any unauthorised attempt to use a different system for school-related communication may be considered a safeguarding concern or a disciplinary matter. If such an attempt is made by a child, it should be reported to the Designated Safeguarding Lead (DSL). If a staff member makes an unauthorised attempt, it should be reported to the Headteacher.

These guidelines are in place to maintain a safe, secure and confidential digital environment for all members of The Children's House School community. We are committed to upholding the highest standards of safeguarding and data protection in all of our communications and data management practices.

Behaviour Principles

The Children's House School is committed to upholding respectful and responsible behaviour in all digital communications and interactions. Please note that the Social Media section of this policy, as well as the school's Acceptable Use Agreements, Behaviour Policy and Staff Code of Conduct, provide more detailed information on these principles. Here are some key behaviour principles:

1. **Appropriate Behaviour**: We expect appropriate behaviour at all times when using our digital systems. This means refraining from sending or sharing materials or language that could be interpreted as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate. Staff members are reminded that their behaviour should never compromise the professionalism of the school or bring it into disrepute.
2. **Data Protection**: In all school communications, we adhere to data protection principles as outlined in the school's Data Protection Policy. This policy is accessible Link to policy page. We stress the importance of using only the authorised systems mentioned in the policy to protect the privacy and security of all school-related data and communications.
3. **Email Use**: Staff are permitted to use the school's email system for reasonable personal use. However, it is essential to be aware that all email activity is monitored, and emails may be subject to review. The same rules of appropriate behaviour apply to personal use. Any emails containing inappropriate language, images, malware, or links to adult sites may be blocked and may not reach their intended recipients. Such instances will be addressed in accordance with the appropriate school policy and procedure.

Maintaining a standard of respectful and responsible behaviour in all digital communications and interactions is crucial to creating a safe and positive online environment within The Children's House School community. These principles guide our approach to digital communication and data protection.

Online Storage or Learning Platforms

The principles governing respectful and responsible online behaviour extend to any online system used for school-related activities. This includes platforms for file storage, data sharing, collaboration, learning, teaching and more. In all cases, the considerations of data protection and cybersecurity are essential. The Children's House School has established clear policies for data protection and cybersecurity, which all staff, governors and volunteers are required to adhere to. You can access these policies via the following links or by referring to the provided sources: Link to policy page.

These policies guide our community in ensuring the secure and responsible use of online platforms, protecting the privacy and integrity of school-related data and activities. Adherence to these policies is essential for maintaining a safe and respectful online environment at The Children's House School.

School website

The Children's House School's website serves as a vital public platform that provides information to both current and prospective members of our school community. The day-to-day responsibility for updating the website content and ensuring compliance with Department for Education (DfE) guidelines has been delegated to the Business manager.

Our website is managed by e4education link, and we take copyright laws seriously. We expect all staff to adhere to copyright regulations, just as any individual or organization should. Copyright infringement can lead to significant fines, with schools in the past facing substantial penalties. When submitting information for the website, please keep the following in mind:

1. Respect Copyright: Uphold copyright law by crediting sources and using materials only with proper permission.
2. Use Public-Domain Resources: Utilize open-access libraries of public-domain images, sounds, and other resources whenever possible. This ensures compliance with copyright regulations.
3. Caution with Internet Content: Merely finding content on platforms like Google or YouTube does not automatically grant permission for use. Always verify copyright status and obtain permission as needed.

If you have any doubts or questions regarding copyright issues, please consult the **Head of IT** for guidance. This responsible approach to copyright ensures that our school website maintains its reputation and respects intellectual property rights.

Digital images and video

When a pupil joins The Children's House School, parents and carers are requested to provide consent for capturing their child's image in photographs or videos. This consent specifies the purposes for which the images or videos will be used and the duration for which the consent remains valid. Parents may grant consent for various purposes, including:

- Displaying images around the school
- Inclusion in the school newsletter
- Use in paper-based school marketing materials.
- In the online prospectus or on the school's websites
- Sharing on social media platforms

Prior to using any photo or video, the staff member responsible for capturing it must consult the latest database, as outlined in the school's data protection policy.

To protect children's privacy, any individuals featured in public-facing materials are not identified beyond their first name. Additionally, photo file names or tags do not include full names to prevent accidental sharing.

All staff members are bound by their employment contracts and the school's Staff Code of Conduct Policy, Mobile Phone and Electronic Device Policy and Acceptable Use Policy, which addresses the use of mobile phones, cameras and all other electronic devices with imaging and sharing capabilities, for taking pictures of pupils, as well as the storage of such media.

All photos are stored on iCloud in compliance with the school's Data Protection Policy's retention schedule. They are deleted at the beginning of each academic year.

Both staff and parents receive annual reminders about the importance of not sharing media without proper permission. This precaution is essential for various reasons, including child protection, data protection, religious or cultural considerations and personal privacy. More information on this topic and a sample letter to parents regarding the capture of photos or videos at school events can be found at parentfilming.lgfl.net.

We actively encourage our pupils to contemplate their online reputation and digital footprint. As responsible adults, we should set a positive example by avoiding oversharing, which could potentially lead to embarrassment later in life. It is not our place to judge what might be embarrassing or not.

Our pupils receive education on online safety, including an understanding of how digital images can be manipulated.

We encourage pupils to refrain from using any social media platforms, such as YouTube, TikTok, Instagram and others. They are educated about the importance of following the guidelines and respecting the age restrictions set by each platform. Furthermore, they learn about the significance of maintaining strict privacy settings to safeguard their personal information and online interactions.

Pupils are educated about the risks associated with sharing information in images, including file names that may disclose the identity and location of others. They also learn about the significance of safeguarding their data and are provided with guidance on what to do if they or a friend experience bullying or abuse.

Social media

Our SM presence

Online Reputation Management (ORM) is a practice that revolves around comprehending about the School online. Nowadays, it's customary for parents to thoroughly research a school online before considering it as an option, and the pre-inspection checks, including monitoring online content, are part of the process.

Negative coverage, no matter how small, can lead to disruptions. Interestingly, up to half of the cases handled by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve concerns about the online reputation of schools and their staff members.

Therefore, we maintain a vigilant watch over our social media presence to stay well-informed about what's being said regarding the school, allowing us to respond to both criticism and praise in a fair and responsible manner.

The Head of Marketing **i**s tasked with the responsibility of managing our social media accounts, and together with the Business Manager, monitors our online reviews and other mentions across the internet.

Staff, pupils' and parents' SM presence

In today's digital age, social media, including popular platforms like YouTube, TikTok, Instagram, Facebook, Snapchat, and more, has become an integral part of our lives. At The Children's House School, we recognize that many parents, staff, and pupils actively use these platforms. However, we expect all members of our school community to maintain a positive and respectful online presence, adhering to the guidelines outlined in our Acceptable Use Policies that every member of our school community commits to.

This positive online behaviour can be simply defined as refraining from making any posts that could be interpreted as bullying, aggressive, rude, insulting, illegal, or otherwise inappropriate. These expectations apply to both public posts and private interactions, such as those within parent chat groups or pages. It is essential that these online interactions align with the same positive conduct expected in face-to-face interactions.

Should parents have concerns about the school, we strongly encourage them to reach out directly through private channels to address their issues. If a matter remains unresolved, we have a structured School Complaints Procedure.

Sharing complaints on social media platforms is unlikely to facilitate resolution and it can cause distress to staff, pupils and parents. It may also adversely affect staff morale and the School's reputation, which is significant for the welfare of the pupils we serve.

While many social media platforms specify a minimum age of 13 (with WhatsApp requiring users to be at least 16), it is not uncommon for issues to arise involving pupils under this age on these platforms. We request that parents respect age restrictions on social media platforms whenever possible and do not encourage or condone underage usage. It's important to note that Online Harms regulations are expected to introduce more stringent age verification measures in the coming years.

Nonetheless, the School faces the challenge of striking a balance between discouraging underage usage and addressing the reality that our pupils and students encounter. Online safety lessons encompass discussions on social media and other online behaviours, emphasizing how to be a positive online friend and how to report instances of bullying, misuse, intimidation, or abuse. However, children often learn most effectively from the examples set by the adults around them.

Parents can play a crucial role by engaging their children in conversations about the apps, websites, and games they use (familiarity with these platforms is not necessary—simply ask your child to explain them to you). Inquire with whom they interact, for how long, and during what hours (particularly late at night or in bedrooms, which can negatively impact a good night's sleep and productive learning at school the next day). You might find the Digital Family Agreement helpful in establishing shared expectations and refer to the Top Tips for Parents poster along with related resources and support available at parentsafe.lgfl.net. Additionally, consider introducing the Children's Commission Digital 5 A Day initiative.

The School maintains an open-door policy. If you have questions or concerns, don't hesitate to reach out.

Although the school has an official X-Twitter and Instagram account, it asks parents/carers not to use these channels, especially not to communicate about their children. Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

*Pupils are not allowed to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media. Pupils are discouraged from 'following' staff, governor, volunteer, or contractor public accounts (e.g., following a staff member with a public Instagram account), as laid out in the AUPs. However, we acknowledge that this can be difficult to control (emphasizing the need for staff to maintain professionalism in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

*Exceptions may be made, e.g., for pre-existing family links, but these must be approved by the Headteacher and should be declared upon the pupil's or staff member's entry into the school.

**Any attempt to do so may be a safeguarding concern or disciplinary matter and should be reported to the DSL (if initiated by a child) or to the Headteacher (if initiated by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute, and the easiest way to avoid this is by maintaining the strictest privacy settings and avoiding inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and must be cautious about ensuring that their personal opinions are not mistakenly attributed to the School, which could harm the school's reputation.

The significance of maintaining appropriate behaviour on social media is underscored by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency due to teaching staff's misuse of social media and technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Camera and Image Policy and permission must be obtained before uploading photographs, videos, or any other information about other people.

The statements within the Acceptable Use Policies (AUPs), which all members of the school community have endorsed, are also applicable to social media activity, as is the school's Data Protection Policy found here.

Device usage

AUPs serve as a crucial reminder for those with access to school devices, outlining the rules regarding the appropriate use of school technology. It's essential to extend these principles to devices used at home, employing them as if they were in full view of a teacher or colleague.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils** are not allowed to bring mobile phones in. Important messages and phone calls to or from parents can be made at the school office, who will also pass on messages from parents to pupils.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and

the school data protection cybersecurity policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off/on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital Images and Video section of this document on page 17; urgent messages can be passed via the school office.

Use of school devices

The use of school devices by both staff and pupils should adhere to the guidelines outlined in the school's Acceptable Use Policies, whether these devices are in use on school premises or at home.

It is imperative that school devices are not utilised in any manner that would violate the terms set forth in the AUPs, the school's Behaviour Policy, or the Staff Code of Conduct.

Access to Wi-Fi is granted to pupils and staff upon signing the AUP, which permits school-related internet usage and limited personal use, all while operating within the framework of the Acceptable Use Policy. It's important to note that all such usage is subject to monitoring.

Additionally, school devices provided to staff and students are limited to the apps and software that have been installed by the school. Any and all usage of these devices, systems, and platforms may be subject to tracking and monitoring.

Trips / events away from school

On school trips/ events away from school, staff mobile devices will be used to keep in touch with the school and to contact parents or other services in case of emergency. Staff will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

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

Appendix – Roles

Please read the relevant roles & responsibilities section from the following pages.
All school staff must read the "All Staff" section as well as any other relevant to specialist roles
Roles:

- All Staff
- Headteacher/Principal
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff Acceptable Use Policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the Designated Safeguarding Lead, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about over blocking, gaps in provision or pupils bypassing protections.

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into the school's overall safeguarding framework.
- Oversee and support the activities of the Designated Safeguarding Lead team, ensuring collaboration with technical colleagues to conduct an online safety audit in alignment with KCSIE, which encompasses the technology used within the school.
- Personally undertake training in both offline and online safeguarding, following statutory guidelines and local safeguarding children partnership support and guidance.
- Ensure that all staff members undergo safeguarding training during their induction, which includes online safety components and regularly receive updates, and confirm their agreement with and adherence to school policies and procedures.
- Ensure that all governors and trustees participate in safeguarding and child protection training, including online safety components, to provide strategic oversight and challenge to policies and practices. Governors

should also receive regular updates on the nature and effectiveness of the school's safeguarding arrangements. (LGfL's Safeguarding Training for School Governors is available to all governors at safetraining.lgfl.net).

- Oversee the school's implementation and effective use of appropriate ICT systems and services, including school-safe filtering and monitoring, and protected email systems. Ensure that all technology, including remote systems, is implemented with a primary focus on child safety.
- Enhance understanding, review, and decision-making related to filtering and monitoring systems, following the new DfE standards. This includes regular communication with technical colleagues and the DSL to comprehend what is blocked or allowed for different user groups and under what circumstances, as specified in KCSIE. This will involve following up on regular checks and annual reviews initiated by the Online Safety Lead and upskilling the DSLs.
- Collaborate closely with the other Designated Safeguarding Leads and DDSLs on all online safety issues that may arise and receive regular updates on school-specific issues and broader policy and practice-related information.
- Provide support to safeguarding leads and technical staff as they review protections for pupils in the home and establish procedures, rules, and safeguards for remote learning.
- Assume overall responsibility for data management and information security, ensuring that the school's data handling adheres to best practices. Work alongside the Data Protection Officer (DPO), DSL, and governors to establish a compliant framework for data storage while ensuring that child protection remains the top priority. Implement data protection processes that facilitate the careful and legal sharing of information.
- Understand and communicate procedures to be followed in the event of a serious online safeguarding incident.
- Ensure that suitable risk assessments are conducted to align the curriculum with the needs of pupils, including the risk of children being radicalised.
- Guarantee that the school website complies with statutory requirements (websiterag.lgfl.net can assist with this).

The Headteacher, plays a crucial role in maintaining a safe online environment within the school community. Her responsibilities cover a wide range of areas, including training, policy adherence, technology oversight, incident response, and risk management. These actions collectively contribute to the school's commitment to providing a secure and nurturing online experience for all students and staff.

Online Safety, Digital Learning & Technical Support Lead:

Key Responsibilities: In addition to the responsibilities outlined in the 'all staff' section, this role includes the following:

- **Alignment with School Policy:** Work closely with the Designated Safeguarding Leads & DDSLs, data protection officer, RSHE lead, and other relevant staff to ensure that school systems and networks are in harmony with school policy. It's essential to prevent conflicts between educational messages and actual practice.
- **Appropriate Language Use:** Use appropriate language and terminology when managing concerns, avoiding victim-blaming language.
- **Collaboration with DSLs and Leadership Team:** Regularly collaborate with the Designated Safeguarding Lead (DSL) and the school's leadership team to provide technical expertise and insights for making strategic decisions related to the safeguarding aspects of technology.
- **Community Engagement:** Promote awareness and commitment to online safety throughout the school community, with a particular focus on parents, including hard-to-reach parents. Dedicated resources can be found at parentsafe.lgfl.net.
- **Consequences and Implications:** Ensure that the above-mentioned stakeholders understand the consequences of existing services and any changes made to these systems. This is particularly important in

terms of access to personal and sensitive records/data, as well as systems like YouTube mode, web filtering settings, sharing permissions for cloud platforms, and more.

- **Continuous Learning:** Receive regular updates on online safety issues and legislation, be aware of local and school trends (examples available at safeblog.lgfl.net) or subscribe to the LGfL safeguarding newsletter.
- **Curriculum Integration:** Ensure that online safety education is integrated across the curriculum in line with statutory RSHE guidance. Utilise resources like the updated UKCIS framework 'Education for a Connected World – 2020 edition.'
- **Cybersecurity and Data Protection:** Manage the school's systems, networks, and devices in line with a strict password policy. Implement systems to detect and address misuse and malicious attacks. Ensure data protection and cybersecurity policies are current, user-friendly and practicable.
- **Daily Safeguarding Responsibility:** Take day-to-day responsibility for safeguarding issues relating to Online Safety and be aware of the potential for serious child protection concerns.
- **Data Management:** Collaborate with the Headteacher, DPO and governors to ensure a compliant framework for data storage, ensuring that child protection remains the top priority, and data protection processes facilitate the careful and legal sharing of information.
- **Delegated Online Safety Duties:** In areas of the curriculum not directly overseen by the DSL but related to online safety (e.g., RSHE - Relationships, Sex and Health Education), the Online Safety Lead is responsible for undertaking regular reviews and ensuring good communication with all relevant colleagues.
- **Documentation:** Maintain up-to-date documentation of the school's online security and technical procedures to ensure transparency and readiness for any audits or reviews.
- **Filtering and Monitoring Oversight:** Take overall responsibility for regular testing of filtering and monitoring systems, logging these in a central location, and keeping reports relating to Filtering and Monitoring. The DSL's responsibility is to work closely with the Online Safety Lead who is also the Technical Support Lead, SLT (Senior Leadership Team), and the online safety governor to assume responsibility for filtering and monitoring. This includes enhancing understanding, reviewing, and driving the rationale behind these systems. Annual checks and annual reviews are conducted, encompassing support for devices used at home.
- **Governor Training:** Together with the Coordinating DSL, ensure that all governors and trustees undergo safeguarding and child protection training, including online safety components during induction to enable them to provide strategic challenge and oversight. This training should be regularly updated.
- **Knowledge Sharing:** Cascade knowledge of online safety risks and opportunities throughout the organisation. Utilise resources available at safecpd.lgfl.net for CPD (Continuing Professional Development).
- **Off-Site Reporting:** Ensure adequate provision for staff to report issues when not in school and for pupils to disclose issues when off-site, especially during isolation or quarantine. This may include using surveys and online forms.
- **Online Safety Audit (Completed Oct 24 and annually hereafter)**: Work closely with DSLs, SLT and staff to complete an online safety audit, including technology in use within the school, as now recommended in KCSIE. This audit should encompass a review of technology, including filtering and monitoring systems, to ensure they align with the new Department for Education (DfE) standards.
- **Policy and Technical Information:** Stay informed about the school's online safety policy and technical information. Your understanding is crucial to fulfilling your online safety role and to inform and update others as needed.
- **Policy Review:** Regularly review and update this policy, other online safety documents, and the strategy on which they are based, in harmony with Risk Assessments for Prevent and relevant policies including Behaviour and Safeguarding. All updates are reviewed by the Chair of the Councill of Management (governing body).
- **Procedures for Online Safety Incidents:** Ensure that all staff members are aware of the procedures to be followed in the event of an online safety incident, and that these are logged similarly to any other safeguarding incident.

- **Regular Communication:** Communicate regularly with SLT and the DSL team to discuss current issues (anonymized), review incident logs and filtering/change control logs, and discuss how filtering and monitoring systems are functioning.
- **Remote Learning:** Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, ensuring that the same principles of online safety and behaviour apply.
- **Reporting and Monitoring:** Report online safety-related issues that come to your attention in accordance with the school's policy. Monitor the use of school technology, online platforms, and the school's social media presence, and promptly identify and report any misuse or attempted misuse as per school policy.
- **Staff Training:** Collaborate with the Coordinating DSL to ensure that all staff members, including supply staff, receive safeguarding and child protection training, including online safety components during induction, and that this training is regularly updated. This should encompass filtering and monitoring components, helping staff understand their roles. All staff must read KCSIE Part 1 and Annex B.
- **Stay Informed:** Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training. (Resources available at safetraining.lgfl.net and prevent.lgfl.net).
- **Support for Filtering and Monitoring:** As per the changes in Keeping Children Safe in Education (KCSIE), this staff member will have a comprehensive understanding of technology's role in safeguarding, especially in filtering and monitoring and will support the safeguarding teams in understanding and managing these systems, including conducting regular reviews and annual checks.
- **Website Compliance:** Collaborate with the School Business Manager to ensure that the school website complies with statutory Department for Education (DfE) requirements.
- **Whole School Approach:** Ensure an effective whole-school approach to online safety in line with KCSIE (Keeping Children Safe in Education) is in place.
- **Zero Tolerance:** Promote a zero-tolerance, whole-school approach to all forms of child-on-child abuse and ensure it is not dismissed as banter, including bullying.

Council of Management Online Safety - Safeguarding Link Governor with Online Safety Responsibilities

Key responsibilities:

- **Policy Approval and Review**: Approve this policy and strategy, and subsequently review its effectiveness. This review can include asking questions outlined in the UK Council for Child Internet Safety (UKCIS) document "Online Safety in Schools and Colleges: Questions from the Governing Board."
- **Governor Training**: Undergo safeguarding and child protection training, including online safety components, at induction, and ensure that all other governors and trustees attend similar training. This training should provide strategic challenge and oversight into policy and practice and should be regularly updated. (LGfL's Safeguarding Training for school governors is available at safetraining.lgfl.net).
- **Staff Training**: Ensure that all staff members receive appropriate safeguarding and child protection training, including online safety, during induction, and that this training is kept up to date.
- **Filtering and Monitoring:** Collaborate closely with the DSL (Designated Safeguarding Lead) on implementing the new filtering and monitoring standards. (Guidance for governors is available at safefiltering.lgfl.net).
- **Community Engagement**: Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- **Strategic Reviews**: Have regular strategic reviews with the online safety coordinator/DSL and incorporate online safety into standing discussions on safeguarding during CoM (governing body) meetings.
- **Data Management**: Collaborate with the Online Safety Leads, DSLs, Headteacher & DPO (Data Protection Officer), to ensure a compliant framework for storing data, prioritising child protection, and facilitating careful and legal information sharing.
- **Staff Training Confirmation**: Check that all school staff have read Part 1 of KCSIE. Ensure that all staff working directly with children have read Annex B.

- **Child Safeguarding in the Curriculum**: Ensure that children are taught about safeguarding, including online safety, as part of a broad and balanced curriculum. The Children's House has a whole-school approach to online safety, with a clear policy on the use of mobile technology and regular reminders to pupils.
- **Curriculum Oversight**: Oversee the delivery of the online safety component of the Computing curriculum in line with the national curriculum. Ensure that students receive a comprehensive education in online safety as part of their computing studies.
- **Collaboration with RSHE Lead**: Collaborate closely with the Headteacher to guarantee a coherent whole-school approach to online safety education. Ensure that both subjects complement each other effectively.
- **Collaboration with DSL/OSL and Staff**: Work closely with the DSLs, DDSLs and OSL (Designated Safeguarding Lead / Online Safety Lead) and all other staff to ensure a shared understanding of the issues, approaches, and messaging related to Computing. This ensures that everyone in the school community is aligned in promoting online safety.
- **Collaboration with the IT and Technical Lead**: Collaborate with the IT Lead to ensure that the online safety components of the computing curriculum are in line with Acceptable-Use Agreements and that the technical infrastructure supports online safety education effectively.

PSHE / RSHE Lead – The Headteacher

Key responsibilities:
General Responsibilities: This role is currently undertaken by the Headteacher. In addition to the responsibilities outlined in the 'all staff' section, this role includes the following:

- **Curriculum Enhancement**: Embed topics related to consent, mental wellbeing, healthy relationships, and staying safe online into the PSHE / Relationships education, Relationships and Sex education (RSE), and Health Education curriculum. Ensure that these subjects cover positive, healthy, and respectful online relationships, the impact of online actions on others, and recognising and demonstrating respectful behaviour online. Teachers should address online safety and appropriate online behaviour in an age-appropriate manner that is relevant to students' lives. Training resources are available at safetraining.lgfl.net.
- **Awareness of Online Risks**: Raise awareness about the risks and challenges associated with recent trends in self-generative artificial intelligence, financial extortion, and sharing intimate pictures online.
- **Underpinning Knowledge and Behaviours**: Ensure that students are taught the underpinning knowledge and behaviours outlined in 'Teaching Online Safety in Schools' in a manner appropriate for their age. The goal is to help students navigate the online world safely and confidently, regardless of the device, platform, or app they use.
- **Assessment**: Assess teaching to identify areas where students may need additional support or intervention. Use various assessment methods, including tests, written assignments, and self-evaluations to track students' progress. LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net can complement the computing curriculum.
- **Collaboration**: Work closely with the DSLs, DDSLs and OSL (Designated Safeguarding Lead / Online Safety Lead) and all other staff to ensure a mutual understanding of the issues, approaches, and messaging within the PSHE / RSHE curriculum.
- **RSHE Policy**: Ensure that an RSHE policy is included on the school website.
- **Collaboration with Computing Lead**: Collaborate with the Computing subject leader to ensure a complementary whole-school approach. Coordinate with other lead staff to ensure a consistent whole-school approach to online safety education.

Class Teachers and Subject Leads

Key responsibilities:
General Responsibilities: In addition to the responsibilities outlined in the 'all staff' section, this role includes the following:

- **Integration of Online Safety**: Actively seek opportunities to integrate online safety into your specific subject or area of responsibility. Pay particular attention to how it can be incorporated into the Relationships, Sex and Health Education (RSHE) curriculum. Serve as a positive role model for both staff and students by demonstrating good practices and attitudes regarding online safety.
- **Reference UKCIS Framework**: Familiarise yourself with the UK Council for Internet Safety (UKCIS) framework "Education for a Connected World" and the guidance provided in "Teaching Online Safety in Schools." Consider how these frameworks can be applied effectively in your subject or area of expertise to promote online safety.
- **Collaboration with DSL/OSL and Staff**: Collaborate closely with the Designated Safeguarding Lead / Online Safety Lead (DSL/OSL) and all other staff members to ensure that everyone comprehends the issues, approaches, and messaging related to online safety in the context of your class or subject.
- **Subject-Specific Planning:** Make certain that subject-specific planning also incorporate an online safety component, ensuring that online safety is woven into the fabric of your subject's teaching and learning.

Data Protection Officer (DPO)

Key responsibilities:
General Responsibilities: In addition to the responsibilities outlined in the 'all staff' section,
this role includes the following:

- **Data Protection Expertise**: Provide data protection expertise, training and support to all staff. Ensure compliance with the Data Protection (DP) and cybersecurity policies and relevant legislation. Verify that these policies align with each other and with this online safety policy.
- **Information Sharing for Child Safety**: Do not prevent or limit the sharing of information when it is necessary to safeguard a child. As outlined in Data Protection in Schools 2023 and Keeping Children Safe in Education (KCSIE) the Data Protection Act 2018 and UK General Data Protection Regulation (GDPR) do not prohibit sharing information for child safety purposes. Fear of sharing information should not impede the obligation to safeguard and promote children's welfare and safety.
- **Record Retention**: Be aware that retention schedules for safeguarding records may be set as 'Very long-term need (until the pupil is aged 25 or older)' and must be passed on to the pupil's next school. Guidance from the NSPCC can be found here.
- **Limited and Monitored Access**: Ensure that all access to safeguarding data is limited appropriately. Implement monitoring and auditing procedures to track access to sensitive information, thereby maintaining data security and privacy.

Volunteers and Contractors (including supply teachers and club leaders, if they use technology)

Key responsibilities:
- **Acceptable Use Policy (AUP)**: Read, understand, sign and adhere to the school's acceptable use policy (AUP). Compliance with this policy is essential for ensuring a safe online environment.
- **Reporting Concerns**: Promptly report any concerns related to online safety, regardless of their perceived significance. Such concerns should be communicated to the Designated Safety Lead within the school.

- **Awareness of Online Safety**: Maintain awareness of current online safety issues and relevant guidance; staying informed about potential risks and safety measures is crucial.
- **Model Safe Behaviour**: Demonstrate safe, responsible and professional behaviours in use of technology while at school or during remote teaching. By modelling these behaviours, volunteers and contractors set a positive example for students.
- **Meeting and Communication Protocol**: Abide by the AUP agreement, which specifies that contractors must not attempt to arrange any meetings, including tutoring sessions, without the full prior knowledge and approval of the school. They should also avoid direct communication with a pupil in a private capacity.

Adherence to these responsibilities helps create a secure and respectful online environment within the school.

Pupils

Key responsibilities:
Pupil Acceptable Use Policy (AUP): Pupils are required to read, understand, sign and adhere to the school's pupil Acceptable Use Policy. This policy outlines the rules and guidelines for safe and responsible technology use while at school or engaging in school-related activities. Adhering to the AUP helps ensure a secure and respectful digital environment for all pupils.

Parents/carers

Key responsibilities:
Parents and carers are responsible for reading, signing and adhering to the school's parental Acceptable Use Policy. They should also familiarize themselves with the pupil AUP and actively encourage their children to follow it. By doing so, parents and carers play a crucial role in promoting safe and responsible technology use among their children and supporting the school's efforts in this regard.

External groups including Parent Associations.

Key responsibilities:

- Sign an Acceptable Use Policy before using technology or the internet within the school.
- Actively support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in your own use of technology, including on social media.
- Refrain from sharing others' images or details without permission.
- Avoid posting negative, threatening or violent comments about anyone associated with the school, including staff, volunteers, governors, contractors, pupils, and other parents or carers.

The Children’s House

Appendix A - Online safety incident record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else’s account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else’s name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

The Children's House

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: X(Former Twitter), Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Lead /DSP/ /Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix B - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety lead or other designated member of staff. This incident log will be monitored at least termly and information reported to SLT and governors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken