

CHIDDINGSTONE NURSERY SCHOOL CIO

Chiddingstone Castle
Hill Hoath Road
Chiddingstone
Edenbridge
Kent TN8 7AD

Telephone:: 01892 871315
Charity Number 1184378



Online Safety, Mobile, Smart Technology, and Social Media Policy

Written by	Mrs Megan Downing - Nursery Leader and DSL Miss Sam Wells - IT Manager
Ratified on behalf of Board of Trustees	September 2026
Date for Review	September 2027
Signed - Co-Chair(s) of Board of Trustees	S.Turpin
Signed - Nursery Leader	M.Downing

This policy will be reviewed and ratified at least annually and/or following any updates to national and local guidance and procedures, and/or any changes to our technical infrastructure.

This policy has been impact assessed by Megan Downing in order to ensure that it does not have an adverse effect on race, gender or disability equality.

Policy Aims and Scope

This policy is based on guidance from the Department for Education (DfE) guidance '[Keeping Children Safe in Education](#)' (KCSIE), '[Early Years Foundation Stage](#)' (EYFS), and the local [Kent Safeguarding Children Multi-agency Partnership](#) (KSCMP) procedures.

This policy has been written by Chiddingstone Nursery School CIO building on Kent County Councils LADO Education Safeguarding Advisory Service, mobile and smart technology, and social media template with specialist advice and input as required.

It takes into account the Department for Education statutory guidance 'Keeping Children Safe in Education, Working Together to Safeguard Children, Early Years Foundation Stage, Ofsted, and the local Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures.

The purpose of this policy is to safeguard and promote the welfare of all members of our nursery community when using mobile and smart devices.

As outlined in our Child Protection policy the Designated Safeguarding Lead is recognised as having overall responsibility for online safety.

Mrs Megan Downing

Our Designated member of staff who co-ordinates online safety issues is:

IT Manager - Miss Sam Wells

Our Data Protection Officer is:

Mrs Victoria Tripp

Mrs Megan Downing works collaboratively with the nursery's IT Manager Miss Sam Wells to implement appropriate security measures and management of the IT systems and devices.

This policy supports the EYFS safeguarding and welfare requirement to have clear policies and procedures for the use of mobile phones, cameras and other devices with imaging and sharing capabilities.

This policy applies to all access to and use of mobile and smart technology on site. For this policy "mobile phone" includes any device with similar functionality, such as the ability to send or receive notification messages, connect to mobile networks or record

images, audio and/or video. This may include but not limited to devices with built in mobile connectivity, smart phones, smart watches, fitness trackers, smart glasses, and other wearable technology.

This policy applies to children, parents/carers and all staff, including the Board of Trustees, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

This policy will be accessible, consistent and straightforward to follow. Expectations will be clearly communicated to staff, parents, and the board of trustees including how the policy will be implemented, how concerns or breaches should be reported, and the possible consequence or sanctions where expectations are not followed.

Chiddingstone Nursery recognises that the use of mobile and smart devices is part of everyday life for many. It is important that children receive consistent messages about the safe use of technology and can recognise and manage the risks posed in both the real and the virtual world.

Links with Other Policies and Procedures

The policy is aligned with our legal duties and safeguarding responsibilities and supports the creation of a calm, safe and supportive environment where children can learn, socialise and seek help without unnecessary distraction, disruption or risk.

This policy links with several other nursery policies and procedures, including, but not limited to; -

- Code of Conducts
- IT Risk Assessments
- Acceptable Use Policies
- Disciplinary Policy
- Child Protection and Safeguarding Policy
- Confidentiality Policy
- Image Use Policy
- GDPR policy

Framework of Risks

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole nursery approach to online safety empowers a nursery community to protect and educate children, staff and parents in their use of technology.

Technology is a significant component in many safeguarding and wellbeing issues. Child abuse can take place online, and/or technology can be used to facilitate offline abuse.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- 1) **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- 2) **Contact:** being subjected to harmful online interaction with other users; 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.
- 3) **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- 4) **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/>).

Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, and the sharing of abusive images and pornography.

Mobile Phone and Smart Device Expectations

Chiddingstone Nursery recognises that mobile and smart technology usage is part of everyday life for many children, staff and parents.

We have a responsibility to provide internet access to support our educational curriculum, and to run the nursery effectively. Children must be empowered to build resilience and to develop strategies to manage and respond to potential risks online.

Personal devices of any kind that are brought onto site are the responsibility of the user. All members our community are advised to:

- take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

- use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal smart devices.

Mobile and smart devices and other forms of smart technology including wearable technology (fitness watches, smart watches, AI smart glasses), are not permitted to be used/worn within nursery. This includes staff. We operate a no mobile or smart devices policy, whereby any mobile and smart devices, including wearable technology are to be kept in the safe box in the office for the duration of their visit.

The sending of abusive or inappropriate messages or content, including via personal devices is forbidden by any member of the nursery community; any breaches will be dealt with in line with our safeguarding, staff code of conduct, parent/staff AUP policies.

All members of the nursery community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our child protection, and other associated policies.

The nursery will ensure that appropriate filtering and monitoring systems are in place on all nursery owned devices, networks and online platforms, in line with statutory safeguarding guidance, including the Prevent Duty and Keeping Children Safe in Education. These systems include virus protection, password protection, sim free devices, BT (our provider) has appropriate systems in place, and locking away phones when not in use.

Nursery Provided Mobile/Smart Devices and Emails.

Members of staff are issued with a work email address to receive nursery related information, which is set up, owned and controlled by the nursery. Once employment has ceased access is removed. Staff should have no expectation that work email accounts are private from the nursery. The Nursery Leader or other authorised person may access and review work email accounts where reasonably required for legitimate nursery purposes, including safeguarding, data protection, investigating concerns or complaints, ensuring compliance with policies, checking appropriate use of the account, or where there is a concern about inappropriate or unauthorised communications. Any access or monitoring will be carried out appropriately and in accordance with UK GDPR, data protection and the nursery's relevant policies and procedures. Unless specific permission from the nursery leader has been sought, under no circumstances are staff permitted to contact nursery families via their work email address.

The Board of Trustees have a separate "Board of Trustees" email group, again set up, controlled and owned by the nursery to conduct nursery related business. This is to

ensure the nursery's GDPR and Data Protection requirements are met. Once an individual has left the committee, access to their nursery email is blocked. Under no circumstances are members of the committee allowed to set up individual email addresses using the Chiddingstone Nursery School name. Doing so would be in breach of this, and other nursery related policies.

Chiddingstone Nursery mobile phones and devices are suitably protected via a password/pin and must only be accessed by members of staff. The main nursery mobile phone is used to store and contact families, used in accordance with Data Protection and GDPR regulations. It is also used to access and play music via an app (appropriate licensing is in place)

The nursery uses sim-free mobile phones (meaning any images/videos cannot be sent to another mobile phone) to record observations for Tapestry. The nursery also uses computers, wi-fi, a sim connected mobile phone, and associated IT systems and networks to conduct nursery business. All of which are suitable protected.

Staff are informed that activity on any nursery owned devices is monitored for safeguarding reasons and to ensure policy compliance. The management team regularly completes spot checks on nursery devices including deleted items.

Nursery devices and IT systems will always be used in accordance with our staff code of conduct, AUP's and child protection policies and other relevant policies.

Staff use of Personal Mobile Phones and Smart Devices

Staff are expected to model safe, responsible and appropriate use of technology at Chiddingstone Nursery. They must comply with this policy at all times and ensure that the use of mobile and smart devices does not distract from, or compromise, the care, privacy, safeguarding or supervision of children.

All staff are expected to uphold and enforce the nursery's mobile phone and smart devices expectations. Staff must not use personal mobile phones or smart devices for personal reasons in front of children during the nursery session. This supports staff to challenge policy breaches consistently and reinforce the expectations placed on children, parents and volunteers.

Staff are not permitted to use their own personal mobile and/or smart technology devices for contacting nursery families.

Any pre-existing links, relationships or circumstances that may compromise this requirement will be discussed with the DSL.

Staff will only use nursery provided sim free mobile phones to take images / videos of children in line with our image use policy. During nursery operating hours staff mobile phones are kept in the office until designated breaks, or in the event of an emergency.

Members of staff will ensure that the use of any mobile and smart devices including personal phones, and other smart devices will take place in accordance with the law, and relevant nursery policies and procedures, including confidentiality, child protection, data protection, AUP and staff code of conduct.

Staff will be advised to ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.

There may be limited circumstances where staff use of a mobile phone or smart device is appropriate for agreed professional, operational or safeguarding purposes, for example to use multi-factor authentication, in response to a family emergency, or to whistle blow. Any such use must be in line with senior management expectations, and must not compromise supervision or safeguarding, and must not undermine the nursery's mobile and smart devices free policy.

If a mobile phone is required for a medical need, such as diabetes, where a device is used to alert a staff member to a reduction in blood sugar levels this will be individually risk assessed and procedures put in place by the nursery leader.

If a member of staff breaches our policy, action will be taken in line with our staff code of conduct and disciplinary policy and procedures.

If a member of staff is thought to have illegal content saved and stored on a personal device or have committed a criminal offence using a personal device, the police will be contacted, and the LADO (Local authority Designated Officer) will be informed in line with nursery policies and procedures. This also extends to illegal and inappropriate content being sent by a staff member.

Security and Management of IT Systems and Applications

Chiddingstone Nursery School CIO is responsible for ensuring we have an appropriate level of security protection procedures in place, to safeguard our systems, and everyone in our nursery community, alongside reviewing the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. This includes: -

- Virus protection.

- Any personal data sent over the internet or taken off site (such as via portable media storage) will be encrypted, and password protected, or accessed via SharePoint.
- Ensure that all staff log off / locks IT devices after use to prevent unauthorised access.
- The nursery has robust risk assessments in place to ensure the safe use of nursery IT devices and systems.
- Passwords are strong and changed regularly.

Personal data will be recorded, processed, transferred, and made available online in accordance with UK GDPR and Data Protection legislation. Full information on managing personal data online can be found in our UK GDPR Data Protection and Information Sharing Policy.

All nursery related passwords are strong to keep files and systems secure. All nursery passwords are kept confidential and never given to a third party. Passwords are changed regularly to reduce the risk of unauthorised access, which may compromise the nursery's IT devices and systems.

Access to the nursery's email systems takes place in accordance with UK GDPR and Data Protection Regulation 2018, and in line with nursery policies, including, AUP, Code of Conduct and Confidentiality.

All members of staff use the nursery email address for any official communication. Work emails may be forwarded where this is necessary for legitimate nursery business, for example to enable the Leader, administrator, or other authorised person to deal with a matter, maintain appropriate records, or respond to safeguarding, data protection, or operational issues. Staff must only forward emails to authorised recipients and must consider whether whole chains are necessary or whether only the relevant information should be shared. Staff must not use work emails to contact parents or other individuals for purposes unrelated to their role and must ensure the Nursery Leader is aware of any such communications. Any electronic communication which contains sensitive, confidential, or personal information will only be sent using secure, encryption and password protection.

The nursery uses the online learning journal Tapestry to share their child's nursery journey with their parents. Parents/carers complete a permission form included in the Admission and Permissions. Written parental consent is obtained before their child/ren's Tapestry account is created.

Children's Education and Use of Mobile and Smart Technology

We have regard to the EYFS safeguarding and welfare requirements, including the Screen Use guidance, which details that children should not be alone when using devices and any screen time should be with the co-engagement of an adult.

Screen time for under 2s should be avoided and children aged 2 - 5 years should be limited to less than one hour per day, this includes time spent on screens at home. Any content should be slow, repetitive and predictable to support children's learning. It should be free of adverts, scrolling and autoplay features.

As an early years settings children do not bring their own personal mobile or screen-based devices into nursery. Where this occurs, staff will discuss this with the parents and manage it on an individual basis. The exception to this would be for a specific SEND or medical need whereby a child uses augmentative and alternative communication devices.

Online safety is embedded throughout the nursery curriculum, to raise awareness of the importance of safe and responsible use of the internet, mobile and smart technology, and to build digital resilience. Children have access to a range of decommissioned technologies to explore, whereby we teach the safe and appropriate use of mobile and smart technology.

We have an embedded and progressive safeguarding education approach by:

- Implementing age-appropriate peer education approaches, for example teaching the children to say, "kind hands", "kind words", "stop, I do not like it".
- Creating a safe environment in which children feel comfortable to say what they feel, i.e. our key person system.
- Making informed decisions to ensure that any educational resources used are appropriate for children.
- Age-appropriate story books
- Reinforce online safety messages whenever devices are used. e.g. who helps keep you safe when you use a screen?
 - only go online with a grown up
 - be kind online **and** keep information about me safely
 - only press buttons on the internet to things I understand

- tell a grown up if something makes me unhappy on the internet
- Staff at Chiddingstone Nursery CIO support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.

Any screen use is limited, planned, age appropriate and clearly linked to intended learning and development aims. We have regard to and support the government guidelines of no more than 1 hour of screen time for the children in our care. We only use reputable sites with a focus on early learning such as CBeebies, and BBC iPlayer (which is set up using nursery information, and contains no ads) alongside exploring different cultures, celebrations, and to enhance our book of the week by watching familiar stories for a limited time. Parents are informed if and when we have complimented our curriculum with technology and of the duration.

We do not use video sharing sites such as YouTube due to the risk of inappropriate content.

Electronic devices, including mobile phones and smart devices, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, Child Sexual Abuse Imagery (CSAM), including nude or semi-nude images, images generated by artificial intelligence, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

Where there are any concerns regarding children, parents/carers of staffs' use of mobile or smart technology or policy breaches, they will be dealt with in accordance with nursery policy and procedures.

Where a concern involves child sexual abuse materials, including nudes or semi-nudes imaged (including AI generated content), or there is suspicion that data or files on a personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, staff will respond in line with the child protection policy and will contact the police immediately.

Visitors use of Mobile and Smart Devices

Parents/carers and visitors are not permitted to use any mobile, smart technology, or wearable technology within the nursery environment. This also extends to Meta AI

glasses which have the capability to record, which again are not permitted to be worn in nursery under any circumstances.

Visitors, including volunteers, Board of Trustees, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our AUP and other associated policies, including child protection and safeguarding.

Staff are expected to challenge visitors if they have concern about their use of mobile and smart devices and will report any breaches to the DSL. The nursery has appropriate signage to inform parents, carers, visitors, and other members of the nursery community that "No Mobile or Smart Devices are to be Used in Nursery."

Visitors' personal devices will be placed in the safe box in the nursery office for the duration of their visit.

Working with Parents / Carers

Chiddingstone Nursery recognises that effective partnership with parents/carers is essential to the successful implementation of this policy. Parents are made aware of the rationale for the policy, including its role in supporting learning, wellbeing and safeguarding.

Parents/carers have an important role in supporting the nursery's mobile phone and smart devices expectations. Parents/carers will be encouraged to discuss the safe use of smart devices at home. Parents/carers are also expected to support the nursery's approach and to work in partnership with staff to reinforce expectations, particularly where policies are breached or concerns arise.

Where individual adaptations or reasonable adjustments are required, for example a SEND or medical need, these will be discussed and agreed directly with parents/carers and recorded appropriately.

The nursery will seek to work constructively with parents/carers to promote children's wellbeing, including supporting safe and responsible use of mobile phones and smart technology beyond the nursery environment.

We actively communicate online safety messages to parents, including the government guidance on screen times via various communication channels and via our website.

Special Educational Needs and Disabilities, Supporting Children with SEND and Vulnerable Children

The internet is an integral part of everyday life for children, and it is important to acknowledge the wide variety of positive opportunities technology provides for young people with SEND; the accessibility of sound, images and video online make it an excellent learning and communication tool, whilst global connectivity enables children with SEND to socialise and access support.

However, children with SEND can be at increased risk online; research suggests they may be more likely than their peers to experience online harms such as scams, cyberbullying, online grooming and exploitation. Children with SEND may also be more likely to have their internet use restricted or be provided with differentiated education, meaning they may have less opportunities to learn through practical experience and/or to develop resilience, or may have less access to support and education which could empower them to use technology safely.

Chiddingstone Nursery School CIO recognises that any child can be vulnerable online, and vulnerability can fluctuate depending on their age, development stage and personal circumstances. However, there are some learners including SEN, looked after children, EAL, or children experiencing trauma or loss, who may be more susceptible or may have less support in staying safe online.

We will ensure that differentiated and appropriate online safety education, access, and support is provided to vulnerable learners. We see the importance of implementing a range of targeted/differentiated online safety strategies to enable children with SEND to access the internet safely, appropriately and learn about staying safe online.

The nursery will seek input from specialist staff as appropriate, including the nursery's SENCO, Miss Sam Wells, and other outside agencies as appropriate. Our nursery website has useful links for parents/carers about supporting children with SEND online.

We develop collaborative understanding of the terminology used to children with SEND, as some children can find abstract language and concepts confusing, so they are provided with clear messages that cannot be open to interpretation.

Cybercrime

Chiddingstone Nursery School CIO is aware of the increasing risk cybercrime has, and is playing on educational settings, and as such we take precautions to ensure our systems and devices stay secure. Staff are aware of their individual responsibilities to ensure they use devices and nursery systems safely. These responsibilities are detailed in this policy, AUP's and staff code of conduct.

Cybercrime is defined as "a criminal activity committed using computers and/or the internet". It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line). Or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include: -

- Unauthorised access to computers (illegal 'hacking')
- Denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources
- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

The government has a nationwide police Cyber Choices programme led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

AI (Artificial Intelligence)

The use of AI (artificial intelligence) is constantly changing and becoming increasingly sophisticated and is embedded in the applications we use every day, and in our smart technology. The use of ChatGPT, Google's Gemini and generative AI continues to grow.

AI is, and can be used in many ways:

- To process and make sense of large amounts of data, identify patterns and follow detailed instructions about what to do with that information.
- To direct the internet to you, based on your search history, e.g targeted advertising.
- To help doctors speed up diagnosis and to identify new treatments.

- Behind voice controlled virtual assistants, such as Apple's Siri, and Amazon's Alexa.

As an early year setting we are acutely aware of the associated safeguarding risks AI pose to children. Generative AI (used to create new content including text and images, which can seem like it has been made by a human), is being used to bully, sexually abuse, exploit, groom, extort, and mislead children.

Policy Monitoring and Review

Chiddingstone Nursery will review this policy at least annually to ensure it remains appropriate, relevant and up to date. The policy will also be reviewed following any changes to national or local guidance, identified safeguarding concerns, or significant changes to the settings use of technology or technical infrastructure.

Technology evolves and changes rapidly, and we are responsible for ensuring the acceptable and safe use of all IT devices, networks, and systems. Ensuring our online safety practice is managed and implemented effectively within the requirements of the law.

The Board of Trustees and the senior leadership team will ensure that appropriate filtering and monitoring systems are in place and regularly reviewed in line with KCSIE and the nursery's safeguarding responsibilities. These arrangements apply to the nursery's devices, networks, and online platforms and are intended to help prevent and/or identify access to harmful or inappropriate content. Any issues identified through monitoring will be addressed through appropriate safeguarding responses and incorporated into action planning.

We monitor internet and technology use taking place via all nursery provided devices and systems and regularly evaluate online safety mechanisms to ensure this policy is consistently applied.

Filtering and Monitoring

Keeping Children Safe in Education states that schools have a responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn and this includes a safe online environment.

In line with our Prevent Duty and the Online Safety Act requirements we will do what we can to limit children, or staff exposure to online risks through filtering and monitoring.

We have a responsibility to block access to illegal and inappropriate content as identified in the Online Safety Act; example include:

- Child Sexual Abuse Material (CSAM)
- Controlling or coercive behaviour
- Extreme sexual violence
- Extreme pornography
- Fraud
- Racially or religiously aggravated public order offences
- Inciting violence
- Illegal immigration and people smuggling
- Promoting or facilitating suicide
- Intimate image abuse
- Selling illegal drugs or weapons
- Sexual exploitation
- Terrorism

Our filtering and monitoring approach has been classified as "low risk". This decision was made because children do not have access to internet-enabled devices.

All nursery owned devices have strict tracking prevention, alongside our internet service provider being BT who is registered with the IWF (Internet Watch Foundation) who collaborate with other technology companies to enhance internet security, and to prevent illegal and inappropriate material online.

This approach is constantly reviewed to ensure our methods are effective and appropriate to limit children's exposure to online risks.

All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring via setting provided devices and networks. This is achieved by annual online safety training for all staff, staff code of conduct and policies and procedures.

We recognise that we cannot rely on filtering and monitoring alone to safeguard children and staff; effective safeguarding practice, robust policies, appropriate behaviour management and regular education/training about safe and responsible use is essential and expected.

Any breaches in our filtering and monitoring system breaches will be reported to the nursery leader and DSL Mrs Megan Downing and to Miss Sam Wells IT Manager. Which will then be dealt with in line with nursery policies, procedures and the law.

Responding to Policy Breaches

All members of the nursery community are informed of the need to report policy breaches or concerns in line with the nursery's existing child protection and safeguarding policies and procedures.

Where parents/carers, children or staff breach this policy appropriate sanctions and/or support will be implemented in line with our disciplinary, acceptable use policies, and code of conducts.

Any concerns will be shared with parents/carers as appropriate. Staff will respond in line with the nursery's child protection and safeguarding policy if there is a concern that a child is at risk of harm.

After any investigations are complete, the Board of Trustees and members from the leadership team will debrief, identify lessons learnt and implement any policy or curriculum changes, as required. We require all staff, parents/carers and children to work in partnership with us to resolve issues.

All members of the nursery community will respect confidentiality and the need to follow the nursery's official procedures for reporting concerns. This has been achieved by all members of the nursery community being informed of our complaints procedure and staff are aware of our whistleblowing procedure.

Staff should consider whether a breach of the mobile phone policy indicates that a child may be suffering, or may be at risk of, harm. Where this may be the case, staff must follow the child protection policy and speak to the DSL without delay. The DSL will consider whether safeguarding action is required, including pastoral support, community-based early help, consultation with relevant services, or a Request for Support to the Front Door Service, in line with local safeguarding procedures.

If we are unsure how to process with an incident or concern, the DSL and/or deputy will seek advice from local authority or other agency in accordance with our child protection policy.

Procedures for Responding to Specific Online Concerns

The following online concerns may not directly affect children of nursery age, but it is important that staff are aware of these potential risks as it may affect their own children, or that of siblings of children that attend the nursery.

Should any of these concerns occur they will be dealt with by the DSL and deputy DSL in accordance with our child protection policy and procedures, and other nursery related policies. The local authority and/or other outside agencies may be contacted for advice.

Additional safeguarding / online concerns include:

- Youth Produced Sexual Imagery
- Upskirting
- Online Abuse and Exploitation. Including CSA (child sexual abuse) and CCE (child criminal exploitation)
- Indecent Images of Children (IIOC)
- Cyberbullying
- Online Hate
- Radicalisation and Extremism
- Child-on-Child Abuse
- County Lines
- Domestic Abuse

Further information and definitions of these additional safeguarding concerns can be found in our child protection policy.

Social Media

We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all children, parents, and staff are protected from potential harm when using social media.

As outlined in our online safety section above, the Designated Safeguarding Lead is Mrs Megan Downing, who is recognised as having overall responsibility for online safety. This policy applies to all uses of social media.

General Social Media Expectations

Chiddingstone Nursery believes everyone should be treated with kindness, respect, and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of the nursery community are expected to engage in social media in a positive and responsible manner.

Inappropriate or excessive use of social media during working hours may result in the removal of internet access or disciplinary action.

We expect members of our nursery community to use social media responsibly and respectfully. Online conduct that is abusive, harassing, threatening, defamatory or otherwise inappropriate may be addressed in line with relevant policies and procedures and, where appropriate, reported to external agencies.

All members of our community are advised not to post or share content that may be considered threatening, hurtful, or defamatory to others on any social media service.

Any concerns regarding the online conduct of any member of staff will be taken seriously. Concerns will be managed in accordance with the appropriate policies and procedures. This also includes concerns relating to online harassment, intimidation or abuse directed towards staff, children or other members of the community.

Chiddingstone Nursery does not have a social media presence.

Staff Use of Social Media

Staff should be mindful of emerging technologies, including artificial intelligence tools and automated features, and must not use these in ways which could compromise confidentiality, professional standards or the safety and wellbeing of children.

Staff are not permitted to use their personal devices during the nursery session to access social media. Staff can however use social media during their designated lunch breaks.

The safe and professional online behaviour is outlined for all members of staff, including volunteers, committee members as part of our acceptable use policies, and associated policies.

The safe and responsible use of social media platforms will be discussed with all members of staff as part of staff induction. Continued advice will be provided and updated via staff in-house training and additional guidance and resources will be shared with staff as required on a regular basis.

Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the nursery. Civil, legal, or disciplinary action may be taken if staff are found to bring the profession into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Members of staff are advised that content shared on social media may be widely viewed, copied or redistributed beyond their control. All members of staff are therefore advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:

- Setting appropriate privacy levels on their personal accounts/sites.
- Being aware of the implications of using location sharing services.
- Using strong passwords.
- Opting out of public listings on social networking sites.
- Ensuring staff do not represent their personal views as being that of the nursery.

Members of staff do not identify themselves as employees of Chiddingstone Nursery on their personal social networking accounts. This is to prevent information being linked with the nursery and to safeguard the privacy of staff members and the wider community. Staff members observe confidentiality and refrain from discussing any issues relating to the nursery, and under no circumstances are nursery children or their families discussed on any platforms of social media.

All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance with nursery policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media as they remain as a permanent digital footprint.

Members of staff will notify the leadership team immediately if they have concerns about content shared online which may impact on their role, the nursery, or the safety and wellbeing of children.

Communicating with Families

Staff will not use any personal social media accounts to contact children or their family members. Staff are advised not to communicate with or add as "friends" of any current or past parents via any personal social media sites.

Any communication from parents/carers received on a staff member's personal social media account will be reported to the DSL Mrs Downing immediately.

Staff are required to declare any existing relationship with a parent on any social media platform to the nursery leader (DSL), Mrs Megan Downing. If ongoing contact

with family members is required once they have left the nursery, staff members will only use official nursery communication devices.

Any complaints about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

Useful Guidance and Links

- IWF work to eliminate child sexual abuse imagery online, preventing the ongoing victimisation of those abused in childhood and making the internet safer for all. [Eliminating Child Sexual Abuse Online | Internet Watch Foundation IWF](#)
- Are you worried about online sexual abuse or the way someone has been communicating with you online? [Make a report](#) to one of CEOP's Child Protection Advisors [CEOP Safety Centre](#)
- Supporting professionals working with children and young people, with any online safety issue they may be having. [Professionals Online Safety Helpline - UK Safer Internet Centre](#)
- If you are worried a child is the victim of cyber-bullying at home or elsewhere, you can speak to the DSL or refer them to help, such as the NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk