



Ditton Church Pre-School



Online/Internet Safety Safeguarding Policy (incl. mobile phones, cameras and social networking)

Policy Statement

Ditton Church Pre-School take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

Key Roles

- Our designated person responsible for co-ordinating action taken to protect children is: Wendy Caldicott
- Our second named designated person responsible for co-ordinating action taken to protect children is: Bev McCrum
- Our named committee representative responsible for safeguarding children is: Tom Kitchen

Procedures and Responsibilities

- The Designated Safeguarding Lead (DSL) has overall responsibility for online safety within the setting but will liaise with other members of staff as necessary.



- The DSL will respond to online safety concerns in line with our child protection and other associated policies, including our Child Protection Policy and our Behaviour Management Policy.
 - Internal sanctions and/or support will be implemented as appropriate.
 - Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

Introduction

- It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. Ditton Church Pre-School will adopt a whole setting approach to internet or online safety which will empower, protect, and educate children and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.
- Ditton Church Pre-School will ensure online/internet safety is considered as a running and interrelated theme when devising and implementing our policies and procedures, and when planning our education approaches, staff training, the role and responsibilities of the DSL and parental engagement.
- Ditton Church Pre-School identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
 - 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.
 - 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.
 - Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
 - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- Ditton Church Pre-School recognises that technology, and the risks and harms related to it, evolve, and change rapidly. We will carry out an annual review of our approaches to online safety, supported by an annual risk assessment, which considers and reflects the current risks our children face online.



The designated responsible person will be informed of any online safety concerns by the DSL, as appropriate. The named committee representative for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

General Principles

- Ditton Church Pre-School uses a wide range of technology. This includes: computers, laptops, tablets and other digital devices, the internet and email systems.
 - Children will never access the internet.
 - Children will never use computers or other devices without direct staff supervision.
 - All setting owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place, as detailed below.
- Ditton Church Pre-School recognises that excessive screen time has been linked to poorer cognitive and behavioural abilities in children. To ensure that screen use involving children is limited, carefully planned and clearly linked to intended learning aims, we will:
 - Only use screens with children where there is a clear educational rationale for doing so and where it extends and enhances learning in a way that is not possible using alternative interactive, screen-free activities.
 - Make sure that screen time it does not displace important activities such as physical activity, time outdoors, story time, and engagement with other children and adults.
 - Check that any digital content is appropriate for early years children; that it is slow-paced, repetitive and predictable; that it is ad-free and that it is free of scrolling or autoplay features.
 - Limit the duration of screen use and work with parents/carers to ensure that children's overall daily screen time does not exceed one hour.
 - Ensure that children never use screens without direct staff supervision.
- Ditton Church Pre-School recognises the specific risks that can be posed by mobile phones, cameras and all other electronic devices with imaging and sharing capabilities that may be used in the setting. This includes any device with functionality or the ability to send or receive messages or notifications, connect to mobile networks, or record images, audio and/or video, for example, but not limited to, devices with built-in mobile connectivity, smart phones, smart watches, smart glasses, fitness trackers and other wearable technology.



- Children will never use electronic devices with imaging and sharing capabilities without direct staff supervision.
 - In accordance with the EYFS Ditton Church Pre-School has appropriate mobile phone, camera and other electronic devices with image and sharing capabilities policy in place, which outline how devices are used in the setting and are laid out below.
- Ditton Church Pre-School recognises that when used safely, effectively and with the right infrastructure in place, generative artificial intelligence (AI) tools have many uses which could benefit our entire community. However, it is important to recognise that AI tools can also pose safeguarding risks as well as moral, ethical and legal concerns. This includes but is not limited to; exposure to inappropriate or harmful content, including bullying, harassment, abuse and exploitation; privacy and data protection breaches/risks; intellectual property infringements and academic integrity challenges and exposure to inaccurate, misleading, or biased content.
 - Children will never have access to AI tools.
 - Ditton Church Pre-School only permits the use of generative AI tools by staff for the purposes of creating learning resources, publicity materials etc. that do not contain any personal information, any material subject to copyright restrictions or any offensive or inappropriate material.
 - Ditton Church Pre-School only permits the use of generative AI tools which have been approved and provided for work and/or educational purposes, following the management team undertaking risk assessments and/or data protection impact assessments prior to use. This includes: list any approved/provided generative AI tools in use. Amend as appropriate to the setting context.
 - Ditton Church Pre-School will respond to any misuse of AI in line with relevant policies, including but not limited to, anti-bullying, behaviour, data protection, complaints and child protection. Amend as appropriate.
- In line with requirements of the Prevent duty, Ditton Church Pre-School will do all we reasonably can to limit children and/or adults' exposure to online risks through the following measures:
 - All staff understand their role, are appropriately trained, follow our policies, processes and procedures, and act on reports and concerns.
 - Children will never access the internet.
 - The DSL has lead responsibility for overseeing and acting on any child protection or safeguarding concerns identified.
 - Ditton Church Pre-School's Internet Service Provider, BT, is a member of Internet Watch Foundation (IWF) and uses IWF services to block access to CSAM.



- Ditton Church Pre-School considers that collectively these measures, and more broadly effective safeguarding practice, robust policies, appropriate behaviour management and regular education/training about safe and responsible use is essential and expected, mitigate the risks relevant to safeguarding and Prevent duties to the extent that the use of filtering and monitoring software is not considered proportionate.
- Ditton Church Pre-School is responsible for ensuring an appropriate level of security protection procedures are in place for Information security and access management, in order to safeguard our systems as well as staff and children. Further information can be found in the GDPR policy.

Training and Education

- Ditton Church Pre-School will ensure that all staff receive online safety training as part of induction and that ongoing online safety training and update for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.
- Ditton Church Pre-School will ensure a comprehensive curriculum response is in place to enable children to learn about and manage online risks effectively as part of providing a broad and balanced age-appropriate curriculum, as detailed below.
- Ditton Church Pre-School will build a partnership approach to online safety and will support parents/carers to become aware and alert of the potential benefits and risks and to reinforce the importance of children being safe online.
- Ditton Church Pre-School will ensure parents/carers understand that children do not have access to the internet while attending the setting.
- Where the setting is made aware of any potentially harmful risks, challenges and/or hoaxes circulating online, national or locally, we will respond in line with the DfE '[Harmful online challenges and online hoaxes](#)' guidance to ensure we adopt a proportional and helpful response.

Information Communication Technology (ICT) Equipment

- Only ICT equipment belonging to the setting is used by staff and children within the setting. This includes tablet computers which are kept on airplane mode to prevent access to the internet. The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- If staff are completing report writing on home computers, they must be encrypted as well as password protected and must only be transferred to the setting via an encrypted memory stick
- All computers have virus protection installed.



- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

Internet Access

- Children do not have access to the internet and never have unsupervised access to computers.
- If staff access the internet for the purposes of promoting children's learning, they will ensure content is age appropriate.
- The designated people have overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age-appropriate way prior to using the internet.
 - only go online with a grown up
 - be kind online
 - 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
 - children are taught about online safety through age-appropriate books, such as 'Penguin Pig', 'Smartie the Penguin', 'It's a Book', 'Chicken Clickin' and 'Dot'
 - information is shared with parents on how to keep their children safe online, via our website, noticeboard and secret Facebook page
- If a second-hand computer or tablet is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it
- All computers or tablets for use by children are located in an area clearly visible to staff.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk
- Suspensions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.
(Although children are not allowed access to the internet in Pre-School staff are alert to comments children may make about something that has happened at home or to an older sibling)



Email

- Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- Staff send personal information via a secure email address and share information securely at all times.

Only leadership staff and administrators will have access to passwords and only these staff will contact parents via email.

Mobile Phones, Smartphones and Smart Devices – Staff and Visitors

- Personal mobile phones, smartphones and all other smart devices with cameras, are not used by our staff whilst supervising children. They will be stored in the designated place (basket in kitchen) and must only be used away from children.
- Our staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- If our members of staff or volunteers take their mobile phones/smartphones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.
- Parents and visitors are requested not to use their mobile phones/smartphones whilst on the premises. Visitors will be advised of a quiet space, i.e. lounge, where they can use their mobile phone, where no children are present

Cameras and Videos

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting.
- Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development, or for displays within the setting, with written permission received by parents
- Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Parents are advised that they do not have a right to photograph anyone else's child or to upload photos of anyone else's children.



- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name.
- Occasionally children may be allowed to use cameras to record things of interest to them, but this would always be under staff supervision.

Social Media

- Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with
- Staff should not accept service users, children and parents as friends due to it being a breach of expected professional conduct.
- In the event that staff name the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users
- Staff observe confidentiality and refrain from discussing any issues relating to work.
- Staff should not share information they would not want children, parents or colleagues to view.
- Staff should report any concerns or breaches to the designated person in their setting.
- Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.
- Our Pre-School Facebook group will be set as a Secret Group and controlled by three administrators: Wendy Caldicott, Pre-School Manager and DSL, and Jane Barwick, Pre-School Administrator. Only current Pre-School children's parents or guardians, grandparents, childminders, committee members and staff will be part of this group. From time to time, we might share photos of Pre-School on this closed site, but photos will only include children where parental permission has been given.

Use and/or Distribution of Inappropriate Images

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed.



- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above)

Further Guidance

- NCA-CEOP: www.ceop.police.uk and www.thinkuknow.co.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Childnet: www.childnet.com
- UK Safer Internet Centre: www.saferinternet.org.uk
- Report Harmful Content: <https://reportharmfulcontent.com>
- Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Internet Matters: www.internetmatters.org
- NSPCC: www.nspcc.org.uk/online-safety
- Get Safe Online: www.getsafeonline.org
- Parents Protect: www.parentsprotect.co.uk
- Cyber Choices: <https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices>
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk

All members of staff in Ditton Church Pre-School are made aware of local support available.

- **Kent Integrated Children's Services/ Children's Social Work Services**
 - [Kent Integrated Children's Services Portal](#) – select 'urgent' if there is an immediate risk/concern
 - Front Door Service: 03000 411111
 - Out of Hours Number: 03000 419191
- **Local Early Help and Preventative Services and Family Hubs**
 - [Early Help and Preventative Services - KELSI](#)
 - [Early Help contacts - KELSI](#)
 - [Kent Family Hubs - Kent County Council](#)
- **Kent Police**
 - 101 or 999 if there is an immediate risk of harm
- **Kent Safeguarding Children Multi-Agency Partnership (KSCMP)**
 - www.kscmp.org.uk
 - 03000 421126 or kscmp@kent.gov.uk
- **Adult Safeguarding**
 - Adult Social Care via 03000 41 61 61 (text relay 18001 03000 41 61 61) or email social.services@kent.gov.uk
- **Kent LADO Education Safeguarding Advisory Service (LESAS) – Support for Kent Children's Workforce**
 - [Local Authority Designated Officer \(LADO\) - Kent Safeguarding Children Multi-Agency Partnership](#)
 - To speak to the LADO regarding an allegation against a member of staff, complete a referral on the [Kent Integrated Children's Services Portal](#).



- To raise a LADO, strategic education safeguarding or online safety enquiry, commission a review or enquiry about bespoke training or other safeguarding products, please use the [LESAS enquiry form](#).
- **UK Council for Internet Safety (UKCIS)**
 - Safeguarding children and protecting professionals in early years settings: online safety considerations

This policy was adopted by the:

Ditton Church Pre-School Management Committee

Date:

September 2026

Signed on behalf of the Management Committee:

Role of signatory:

Chair of Management Committee

Next review date:

April 2027