

Ditton Lodge Primary School



Online Safety Policy

|  |  |  |
| --- | --- | --- |
| **Approved by Full Governing Body** | | **Date: 16th March 2021** |
| **Last reviewed on:** | March 2021 |  |
| **Next review due by:** | March 2023 |  |

**Contents**

* The background to this policy
* Rationale
* The online safety curriculum
* Continued Professional Development
* Monitoring, and preventing online safety incidents
* Responding to online safety incidents
* Appendices (including AUPs)

**Background to this policy:**

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

* The policies and practice embedded in our school and followed by the whole school community
* The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to online safety incidents
* A progressive, relevant age appropriate online safety curriculum for all pupils

Online safety in schools is primarily a safeguarding and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

* Safeguarding and Child Protection
* Personal Social and Health Education (PSHE)
* Safer Working Practices
* Data Protection / GDPR Policy
* Anti-Bullying Policy
* School Complaints Procedure
* [Cambridgeshire Progression in Computing Capability Materials](http://www.ccc-computing.org.uk)
* Whistle Blowing Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

* The development of our safety policy involved:
  + The Headteacher
  + The Designated Safeguarding Lead
  + The Computing Subject Leader
  + Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
  + The governor responsible for Safeguarding

It was presented to the governing body on and ratified on *23 March 2021* and will be formally reviewed in March 2022.

* This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school’s use of technology. It has been shared with all staff via email and a staff meeting and is readily available on the school network and website, and has also been made available to parents via the website.
* All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school’s systems (see appendices). As Online safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

**Rationale:**

* At Ditton Lodge Primary School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the ‘3 C’s’ **Contact**, **Content** and **Conduct** (Livingston and Haddon) and may include:

* Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
* Unauthorised access to / loss of / sharing of personal information
* The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
* The sharing / distribution of personal images without an individual’s consent or knowledge
* Inappropriate communication / contact with others
* Cyber-bullying
* An inability to evaluate the quality, accuracy and relevance of information on the internet
* Plagiarism and copyright infringement
* Illegal downloading or streaming of music or video files
* The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

* Staff laptops, iPads and also desktops in the office and classrooms including staff level internet access, server access and access to MIS systems.
* Staff have access to school systems (cloud storage of school files) and some staff have access to MIS Systems beyond the school building. Staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
* Class cameras, iPads and other peripherals such as visualisers and Interactive Whiteboards

Pupils:

* Curriculum laptops / iPads / Chromebooks including filtered access to the Internet and pupil level access to areas of the school network
* Cameras and peripherals including programming resources (Beebots, control equipment, class cameras etc.)

**The online safety curriculum:**

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing which states that:

* **At KS1:** use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
* **At KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Ditton Lodge Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils’ ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

* Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform, (e.g. GSuite and O365)
* Our programme for online safety education is evidenced in teachers’ planning both as discrete, embedded and continuous activities.
* Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.

**Continued Professional Development:**

* Staff at Ditton Lodge Primary School receive up-to-date information and training on online safety issues in the form of staff meetings and updates from the school’s Computing Lead and Designated Safeguarding Leads, as well as training from external providers where appropriate.
* Nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school’s approach, policies and practice.
* New staff receive information on the school’s acceptable use policy as part of their induction, including advice on protecting their professional reputation online in line with teacher standards.
* All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

**School website:**

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information our pupils and parents, promote the school to prospective ones and publish as a minimum the statutory information required by the Department for Education.

In conjunction with a range of online services, our school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both for in school and at home.

The school has clear expectations that its website and digital are maintained, are effective, and do not compromise the safety of the pupils or staff.

**Parents/Carers Roles and Responsibilities**

Parents/Carers have a crucial role in educating and protecting pupils when using digital technologies. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and through social media and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

* Newsletters sent home from the school, following a programme of information sharing (see Appendix 2)
* High profile events such as Safer Internet Day
* The distribution of relevant guidance should a particular topic/theme be highlighted by pupils in school
* Prompt discussions with parents/carers if concerns arise.

**Monitoring, and averting online safety incidents:**

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children’s online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school’s technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority’s Education ICT Service. Safeguards built into the school’s infrastructure include:

* Secure, private CPSN provided internet connection to each school with a direct link to the National Education Network.
* Managed firewalling running Unified threat management (UTM) that provides Restrictions on download of software, apps and file types from known compromised sites.
* Base line and optional enhanced filtering.
* Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested.
* Antivirus package provided as part of CPSN Connection.
* Wireless networks installed by Unity Schools Partnership ICT Department are encrypted to industry best practice standards and the wireless key is kept securely by the school office.

Staff also monitor pupils’ use of technology and, specifically, their activity online.

* Pupils’ use of online services (including the World Wide Web) are supervised in school at all times.
* Staff are also able to monitor pupils’ activity in the (e.g. GSuite and O365) online environment, allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

* All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.
* Visitors to the school can access part of the school systems using a generic visitor login and password.
* The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
* School staff and pupils are not permitted to connect personal devices to the school’s wireless network.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

**Responding to online safety incidents:**

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

* Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
* If an online safety incident occurs, Ditton Lodge Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school’s AUPs – see appendix).

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

* With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

*NB: In our school, the likelihood of these types of instances occurring are already reduced as we don’t allow pupils to use personal devices in school.*

**Children and online safety away from school**

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Procedures and where appropriate referrals should still be made to children’s social care and, as required, the police.

Online teaching should follow the same principles as set out in the Trust’s code of conduct and acceptable use of ICT policy.

Ditton Lodge Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

* Parents/Carers should be present in the background when pupils are talking to staff.
* Staff and children must wear suitable clothing, as should anyone else in the household.
* Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
* The live class should be recorded so that if any issues were to arise, the video can be reviewed. The recording should be stored on the school’s network in an area that can only be accessed by those staff who need to. It will be retained for a year, after which time it will be deleted.
* Live classes should be kept to a reasonable length of time, or the streaming may prevent the family ‘getting on’ with their day.
* Language must be professional and appropriate, including any family members in the background.
* Staff must only use platforms specified by senior managers and approved by the Trust’s Head of IT to communicate with pupils
* Staff should record, the length, time, date and attendance of any sessions held.

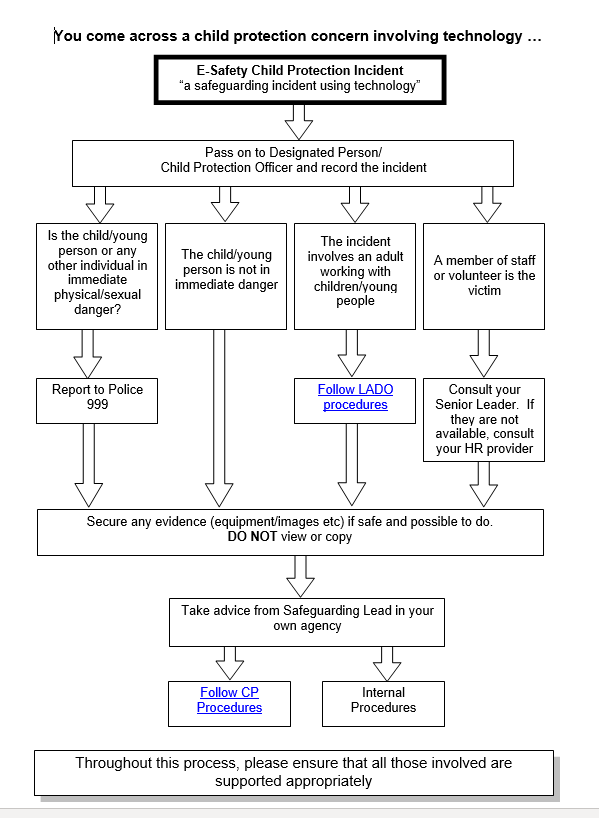
Ditton Lodge Primary School will ensure children who are being asked to work online know how they can raise any concerns whilst online. As well as reporting routes back to the school, age appropriate practical support is available from:

* [Childline](https://www.childline.org.uk/?utm_source=google&utm_medium=cpc&utm_campaign=UK_GO_S_B_BND_Grant_Childline_Information&utm_term=role_of_childline&gclsrc=aw.ds&&gclid=EAIaIQobChMIlfLRh-ez6AIVRrDtCh1N9QR2EAAYASAAEgLc-vD_BwE&gclsrc=aw.ds) - for support
* [UK Safer Internet Centre](https://reportharmfulcontent.com/) - to report and remove harmful online content
* [CEOP](https://www.ceop.police.uk/safety-centre/) - for advice on making a report about online abuse

Support for parents and carers to keep their children safe online includes:

* [Internet matters](https://www.internetmatters.org/?gclid=EAIaIQobChMIktuA5LWK2wIVRYXVCh2afg2aEAAYASAAEgIJ5vD_BwE) - for support for parents and carers to keep their children safe online
* [London Grid for Learning](http://www.lgfl.net/online-safety/) - for support for parents and carers to keep their children safe online
* [Net-aware](https://www.net-aware.org.uk/) - for support for parents and careers from the NSPCC
* [Parent info](https://parentinfo.org/) - for support for parents and carers to keep their children safe online
* [Thinkuknow](http://www.thinkuknow.co.uk/) - for advice from the National Crime Agency to stay safe online
* [UK Safer Internet Centre](https://www.saferinternet.org.uk/advice-centre/parents-and-carers) - advice for parents and carers

**Appendix 1**

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.

**Appendix 2**

|  |  |
| --- | --- |
| **Week** | **Resource** |
| 1 | National Online Safety Guide: What parents need to know about online content. 10 tips to keep your children safe  https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-online-content-10-tips-to-keep-your-children-safe-online |
| 2 | National Safety Online Guide: What parents need to know about age ratings  https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-age-ratings |
| 3 | National Online Safety Guide: What parents need to know about search engines  https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-search-engines |
| 4 | National Online Safety Guide: Children’s Devices and Online Safety  https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-children-s-devices |
| 5 | National Online Safety Guide: What parents need to know about games consoles  https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-games-consoles |
| 6 | National Online Safety Guide: Online Safety Guide to Home Internet Controls  https://nationalonlinesafety.com/guides/a-free-guide-to-home-internet-controls-for-parents-carers |
| 7 | National Online Safety Guide: Social Media Online Tips  https://nationalonlinesafety.com/guides/12-social-media-online-safety-tips |
| 8 | National Online Safety Guide: 7 Questions to Start a Conversation about Online Safety  https://nationalonlinesafety.com/guides/7-questions-to-help-you-start-a-conversation-with-your-child-about-online-safety |
| 9 | National Online Safety Guide: Guide to Youtube Kids  https://nationalonlinesafety.com/guides/8-things-parents-need-to-know-about-youtube-kids |
| 10 | National Online Safety Guide: Guide to Roblox  https://nationalonlinesafety.com/guides/roblox-parent-s-guide |
| 11 | National Online Safety Guide: Guide to Minecraft  https://nationalonlinesafety.com/guides/minecraft-parent-s-guide |
| 12 | National Online Safety Guide: Guide to TikTok  https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-tiktok |
| 13 | National Online Safety Guide: Guide to WhatsApp  https://nationalonlinesafety.com/guides/whatsapp-online-safety-guide-for-parents |
| 14 | National Online Safety Guide: Guide to Instagram  https://nationalonlinesafety.com/guides/instagram-parent-s-guide |
| 15 | National Online Safety Guide: Guide to PS4  https://nationalonlinesafety.com/guides/ps4 |
| 16 | National Online Safety Guide: Guide to Xbox One  https://nationalonlinesafety.com/guides/xbox-one |
| 17 | National Online Safety Guide: Mental Health and Social Media  https://nationalonlinesafety.com/guides/social-media-mental-health-the-positive-and-negative-impacts |
| 18 | National Online Safety Guide: What Parents Need to Know About Friends and Followers  https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-friends-followers |
| 19 | National Online Safety Guide: Guide to Fortnite Battle Royale  https://nationalonlinesafety.com/guides/fortnite-battle-royale-online-safety-guide |
| 20 | National Online Safety Guide: Guide to Live Streaming  https://nationalonlinesafety.com/guides/live-streaming-guide-for-parents |
| 21 | National Online Safety Guide: Guide to Online Bullying  https://nationalonlinesafety.com/guides/what-school-staff-need-to-know-about-cyberbullying |
| 22 | National Online Safety Guide: Safer Apps and Games for Chilldren  https://nationalonlinesafety.com/guides/suggested-apps-and-games |

**Appendix 3**

**Remote Learning Expectations**

This document sets out how remote learning will be delivered at Ditton Lodge Primary School

**Staff code of conduct**

When providing remote learning our staff will follow this code of conduct:

1. 1:1s should be avoided where possible; a parent/carer should be present for the duration of the session (in the locality).
2. Staff should not behave any differently towards pupils compared with when they are in school. They must never attempt to arrange any meeting, including additional sessions, without the full prior knowledge and approval of the school, and should never do so directly with a pupil.
3. Staff should make reasonable adjustments and specific arrangements for SEND pupils remotely as you would in the classroom.
4. Staff should only use platforms specified by the school. They should not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without prior approval.
5. All 1-2-1 or small group lessons (with 3 or less children) should be recorded (including drop ins with one member of staff) so that if any issues arise the video can be reviewed. The recording must be stored on your Google Drive. It will be retained for a year, after which time it should be deleted. Staff must not take secret recordings or screenshots of themselves or pupils during sessions.

Instructions for recording remote learning:

On the tool bar at the bottom of Google Meets (where the ‘raise hand’ button is, there are three dots. Click on those. A menu should appear with the option to ‘Record Meeting’. Click on this. A message will appear asking you to start the meeting. There will then be a short delay before the meeting records. Make sure the children ‘pin’ you to minimise the amount of time children’s faces are on screen.

At the end of the meeting, go back to the same menu and click ‘Stop Recording’.

All meetings will be stored in your Google Drive. Google Drive will automatically create a folder for recorded meetings.

1. Staff should conduct any remote learning sessions in a professional manner, as if they were in school. This includes being suitably dressed, using professional and appropriate language and not being in a bedroom or bathroom. Where the use of a bedroom is unavoidable, it should be impossible to tell that it is a bedroom, even if the camera slips. The camera view should not include any personal information or inappropriate objects and the background should always be blurred/changed.

Instructions for blurring backgrounds:

On the tool bar at the bottom of a Google Meets (where the ‘raise hand’ button is, there are three dots. Click on those. A menu should then appear with the option to ‘Change Background’. Click on that. You should then see a range of backgrounds to choose from. The two buttons which look like a head with dots around it are the blurring options.

1. If anything inappropriate happens - or anything which could be construed in this way – staff must immediately inform their line manager and record on CPOMS. This is to protect staff and pupils.
2. Staff should look out for signs that a child may have been harmed or be at risk of harm, as they would if they were in school. Any concerns or disclosures must immediately be passed on to the Designated Safeguarding Lead in the pupil’s school or, in their absence, a deputy designated safeguarding lead, in line with the school’s child protection procedures.

**What we expect from parent(s)/carer(s)**

To keep your child safe and ensure they get the most from remote learning, we expect you to:

1. Where possible be present for the duration of the session. Try to be in the room for all sessions, especially for younger children.
2. If your child has additional needs and attends mainstream school please liaise with the schools SENCO regarding what is working well or needs adjusting for your child. If your child attends a specialist provision (school or hub) then you will receive additional guidance from them and are invited to be in close contact regarding your child’s specific needs.
3. Make sure your child does not join a session from a bedroom or bathroom. If joining a session from a bedroom is unavoidable, point the camera away from beds and any personal information.
4. All children should be supported to blur or change the background where possible.

Instructions for blurring backgrounds:

On the tool bar at the bottom of a Google Meets (where the ‘raise hand’ button is, there are three dots. Click on those. A menu should then appear with the option to ‘Change Background’. Click on that. You should then see a range of backgrounds to choose from. The two buttons which look like a head with dots around it are the blurring options.

1. Make sure your child, and anyone else who might be seen during the session, wears suitable clothing and is fully dressed.
2. Make sure that your child’s language, and that of anyone in the background, is appropriate.
3. Do not take secret recordings or screenshots of the member of staff or other pupils during the session(s).
4. Make sure your child knows they can tell you if they are asked to keep a secret or anything happens or is said that is strange or makes them feel uncomfortable, scared or upset.

**If you have any safeguarding concerns about the member of staff, report them immediately to the Headteacher at your child’s school.** The Headteacher will follow the guidance in part four of [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), which deals with allegations of abuse made against teachers and other staff.

**What we expect from pupils**

1. Attend all lessons on time with a positive attitude.
2. Always wear suitable clothing when you are joining a session.
3. Always blur your background so nothing personal is on show behind you.
4. Be polite and respectful of others in the lesson just as you would be in school.
5. Follow your teacher’s instructions if you have a question or answer you would like to share.
6. Let your teacher know if you are finding the work too hard or too easy.
7. If you have additional needs and are worried that you can’t access or understand some of the home learning tasks, or are not receiving the feedback you need, let your teachers and family members know.
8. Never record or take pictures of anyone in your lesson.

Let your parent/carer, teacher or Headteacher know straight away if you are asked to keep a secret or anything happens or is said that is strange or makes you feel uncomfortable, scared or upset.