

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Introduction

## Key people

Cononley Primary School	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Catherine Pickles
	Deputy Designated Safeguarding Leads / DSL Team Members	Jaki Fraser Lucy Holmes
	Link governor for safeguarding Link governor for Monitoring and Filtering	Katie Mason Rachel Price Waite
	Curriculum leads with relevance to online safeguarding and their role [ e.g. PSHE/RSHE/RSE/Computing leads ]	Ross Milner (Computing Lead) Jaki Fraser (PSHE Lead)
	Network manager / other technical support	NYES Digital
	Date this policy was reviewed and by whom	March 2024
	Date of next review and by whom	March 2025

## What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

## Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

## Who is in charge of online safety?

KCSIE makes clear that “the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety).” The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

## What are the main online safety risks in 2023/2024?

### Current Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students: children have made unsafe searches on school devices and used social media (under the recommended age) in a way that has not been safe at home. We have also had cases of children using Snapchat to film videos of fights and to threaten other children.

Nationally, some of the latest trends of the past twelve months are outlined below. These should be reflected in this policy and the acceptable use agreements we use, and seen in the context of the 4 Cs – content, contact, conduct and commerce (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

We may be updating this policy during the year to reflect any changes resulting from the Online Safety Bill being passed into law.

Self-generative artificial intelligence has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home.

Children increasingly spend more time online and are therefore exposed to all manner of online harms as families have had to cut back on leisure activities and the public provision of free activities for young people has reduced further.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases. At Cononley Primary School we carry out annual pupil surveys to find out about our children's access to the internet so that we can respond accordingly.

In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed the ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys over the past year which schools have had to counter.

From the many schools that LGfL spoke to over the past year, there was a marked increase in the number of schools having issues with fights being filmed and shared, a disturbing increase in the cases of self-harm and sexual abuse being coerced with threats of violence (many even in primary schools).

There has been a significant increase in the number of fake profiles causing issues in schools, both for schools – where the school logo and/or name have been used to share inappropriate content about students and also spread defamatory allegations about staff, and also for students, including where these are used to bully others (sometimes even pretending to be one student to bully a second student). At Cononley Primary School, we have not yet experienced fake profiles being used, but we are alert to the fact that this happens in other schools and could happen here.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school

## Contents

Introduction	1
Key people	1
What is this policy?	1
Who is it for; when is it reviewed?	1
Who is in charge of online safety?	2
What are the main online safety risks in 2023/2024?	2
How will this policy be communicated?	4
Contents	4
Overview	7
Aims	7
Further Help and Support	7
Scope	8
Roles and responsibilities	8
Education and curriculum	8
Handling safeguarding concerns and incidents	10
Actions where there are concerns about a child	11
Sexting – sharing nudes and semi-nudes	14
Upskirting	15
Bullying	15

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

Child-on-child sexual violence and sexual harassment	15
Misuse of school technology (devices, systems, networks or platforms)	16
Social media incidents	16
Data protection and cybersecurity	17
Appropriate filtering and monitoring	17
Messaging/commenting systems (incl. email, learning platforms & more)	19
Authorised systems	19
Behaviour / usage principles	20
Online storage or learning platforms	21
School website	21
Digital images and video	21
Social media	22
Our SM presence	22
Staff, pupils' and parents' SM presence	23
Device usage	24
Personal devices including wearable technology and bring your own device (BYOD)	24
Use of school devices	25
Searching and confiscation	25
Appendix – Roles	26
All staff	26
Headteacher – Catherine Pickles	26
Designated Safeguarding Lead / Online Safety Lead – Catherine Pickles	27
Governing Body, led by Safeguarding Link Governor – Katie Mason, and Filtering and Monitoring Governor, Rachel Price Waite.	29
PSHE / RSHE Lead – Jaki Fraser	30
Computing Lead – Ross Milner	31
Subject / aspect leaders	31
Network Manager/other technical support roles – NYES Digital / LA Safeguarding Officer	32
Data Protection Officer (DPO) – Veritau	33
Volunteers	33
Pupils	34

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

Parents/carers	34
External groups including parent associations –Friends of Cononley School	34

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Overview

### Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Cononley Community Primary School's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

## Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. Catherine Pickles (DSL and Headteacher) will handle referrals to local authority multi-agency safeguarding team (MAST) and she also handles referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

Beyond this, [reporting.lgfl.net](https://reporting.lgfl.net) has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people. Training is also available via [safetraining.lgfl.net](https://safetraining.lgfl.net)

## Scope

This policy applies to all members of the Cononley Primary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

## Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should **read the relevant section in Annex A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

In 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

## Education and curriculum

It is important that schools establish a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools (DfE January 2023) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

to the specific needs of pupils, including vulnerable pupils – dedicated training around this with curriculum mapping for RSHE/PSHE and online safety leads is available at [safetraining.lgfl.net](https://safetraining.lgfl.net)

RSHE guidance also recommends schools assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress.”

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Personal, Social, Health and Economic Education (PSHE) which includes Relationships, Health and Sex Education (RSHE)
- Computing

At Cononley Primary School, we also use simple quizzes and surveys such as the LGfL’s Safe Skills Online Safety Quiz which is linked to statements from the UKCIS Education for a Connected World statements, enabling teachers to monitor progress throughout the year and identify areas which require further development.

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites. “Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online” (KCSIE 2023).

At Cononley Primary School, we use Smoothwall to filter and monitor online activity. NYES Digital provide technical support to ensure that Smoothwall runs effectively. Parents and carers have been informed about Smoothwall in our weekly bulletin.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. [saferesources.lgfl.net](https://saferesources.lgfl.net) has regularly updated theme-based resources, materials and signposting for teachers and parents.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

At Cononley Community Primary School we recognise that online safety and broader digital resilience: our computing scheme, Purple Mash, and PSHE/RSHE scheme (Kapow) incorporate the framework 'Education for a Connected World – 2020 edition' from UKCIS (UK Council for Internet Safety).

This is done within the context of an annual online safety audit, which is a collaborative effort led by the DSL (Catherine Pickles) and the Computing Lead (Ross Milner) and monitored by the governing body, led by the Safeguarding Governor, Katie Mason.

## Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE/RSHE).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the designated safeguarding lead (Catherine Pickles) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Child Protection Policy
- Anti Bullying Policy (includes the procedures for Child-on-Child Abuse)
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment
- Privacy Agreements
- Information Policy

This school commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

Any concern/allegation about staff misuse is always referred directly to the Headteacher/ DSL (Catherine Pickles), unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline: 0800 028 0285

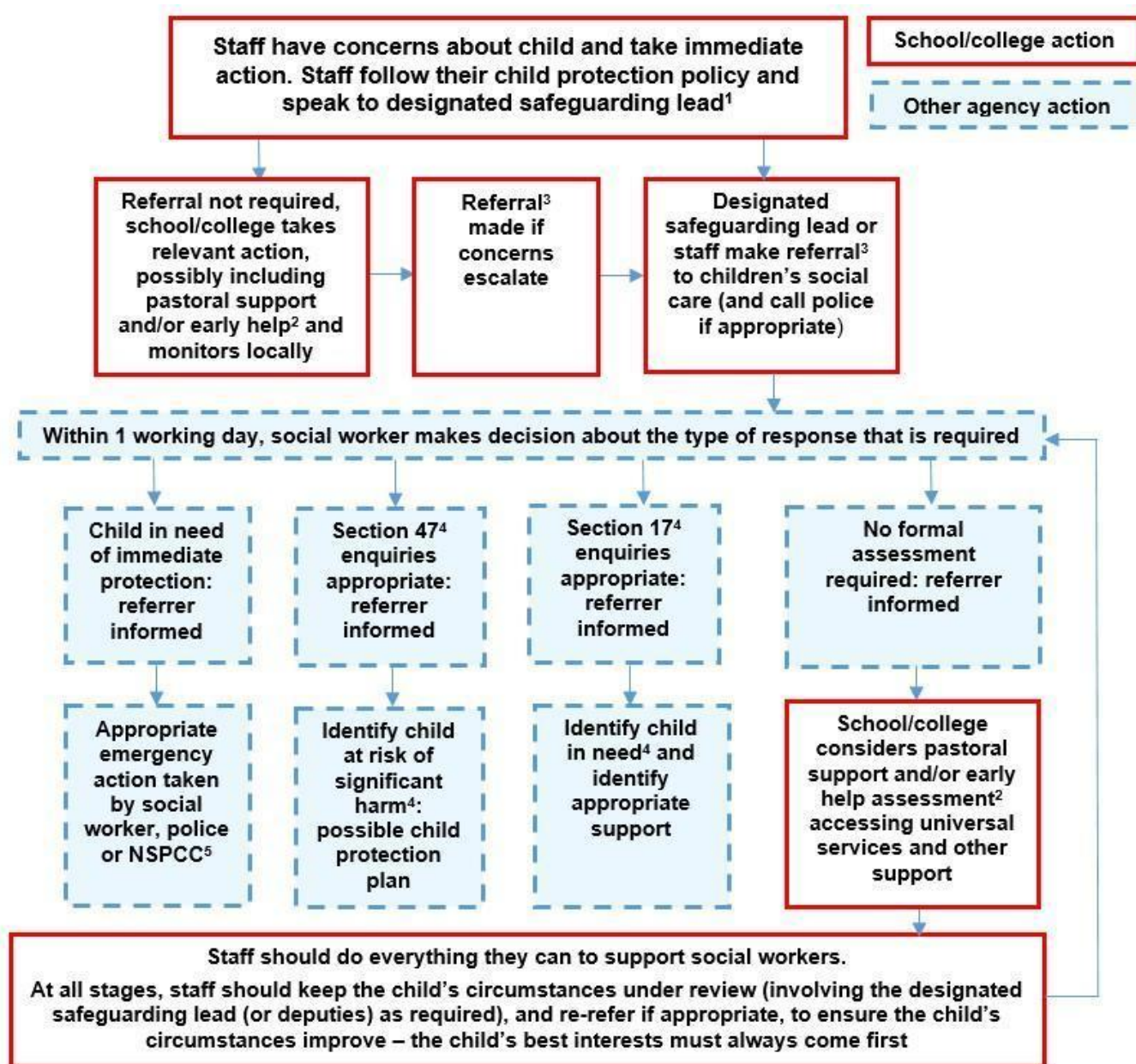
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance [Behaviour in Schools, advice for headteachers and school staff](#) September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

## **Actions where there are concerns about a child**

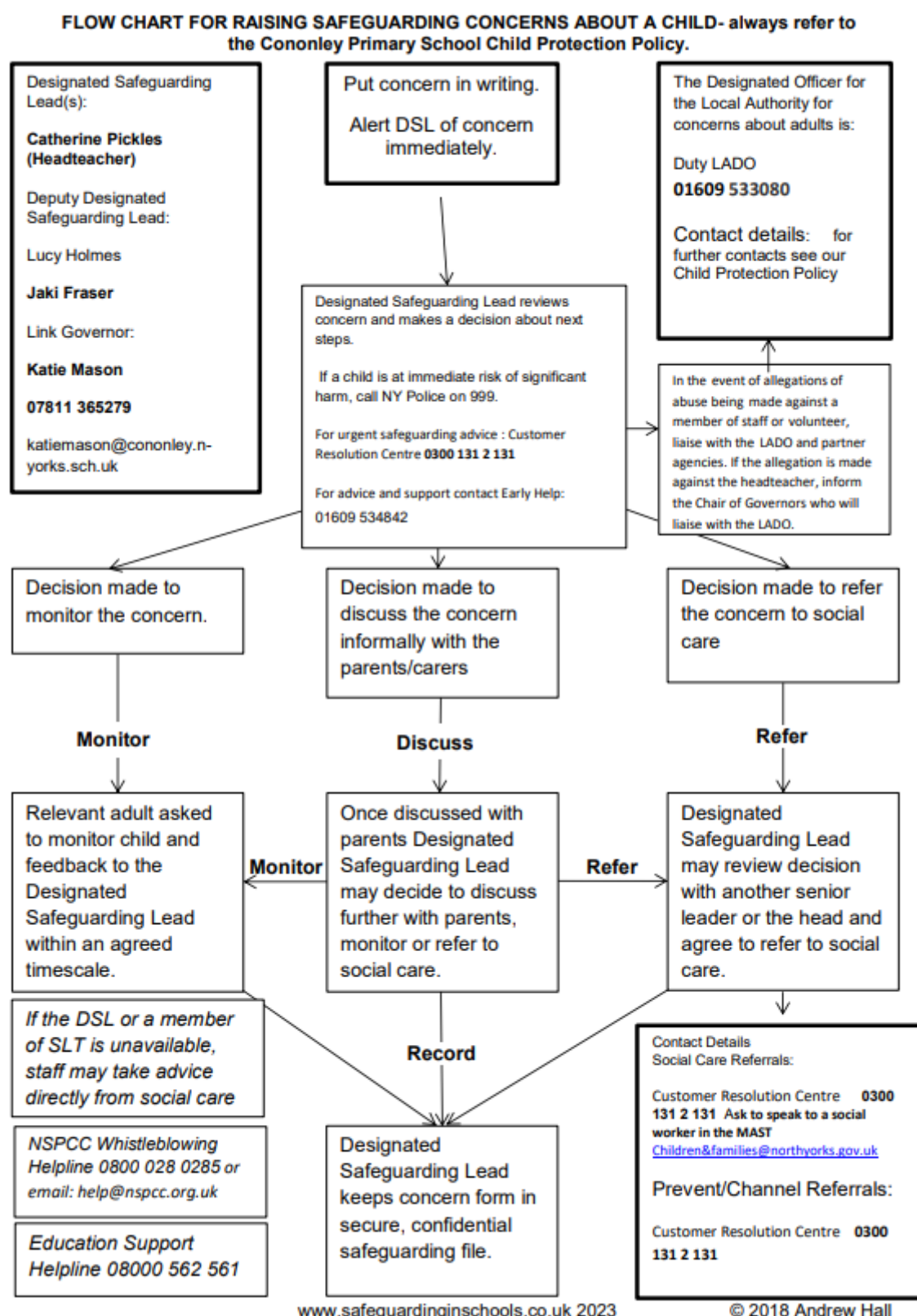
The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT



# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Cononley Primary School Safeguarding Flow Chart



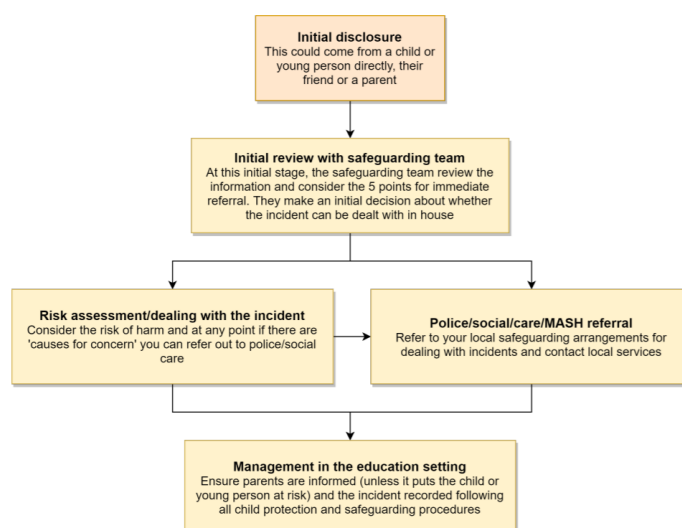
# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#) to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved.



**\*Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at [sexting.lgfl.net](https://sexting.lgfl.net)

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

## Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. To read our Anti Bullying Policy, please see our school website:

<https://www.cononleyprimary.org.uk/key-info/school-policies/policies/anti-bullying-policy>

It is important to be aware that in the past 12 months there has been an increase in anecdotal reports of fights being filmed and fake profiles being used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at [bullying.lgfl.net](https://bullying.lgfl.net)

## Child-on-child sexual violence and sexual harassment

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment'; all staff have read this document and take part in safeguarding training throughout the year, which includes updates about child on child sexual violence and sexual harassment.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL, Catherine Pickles, who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policies and Internet Safety Rules for pupils, as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff Code of Conduct.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

The new responsibilities for filtering and monitoring, led by the DSL and following the new DfE standards, may mean that more such incidents will be discovered in the coming year.

## Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Cononley Primary School community. These are also governed by school Acceptable Use Policies and the Parent and Carer Behaviour Policy.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

Parents and carers should take care when posting messages on social media. Parents are expected to treat everyone with respect and professionalism – even on social media - and adults should set a good example to their children and other pupils. Do not use social media to criticise the school or its staff or pupils or make inappropriate comments.

In the event that any pupil or parent/carer of a pupil is found to be posting inappropriate comments on social media, they will be reported to the appropriate 'report abuse' section of the social media site and consideration will be given to taking further action. Making potentially defamatory, offensive or derogatory comments about others on social media could have legal implications. In addition, threats

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

of violence can lead to a criminal action. The school will also expect any pupil or parent/carer to remove such inappropriate comments immediately.

## Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements which can be found here: <https://www.cononleyprimary.org.uk/key-info/school-policies>

It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

At Cononley Primary School, the following data security products are used to safeguard children, which in turn supports the integrity of data and data protection: Sophos Anti-Virus, Firefox, Egress, Smoothwall.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

## Appropriate filtering and monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" webfiltering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

As schools get to grips with these new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via email to the DSL / Headteacher Catherine Pickles ([headteacher@cononley.n-yorks.sch.uk](mailto:headteacher@cononley.n-yorks.sch.uk)) and will be asked for feedback during the school year.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at <https://safefiltering.lgfl.net> and training is provided for all staff / safeguarding teams / technical teams as appropriate.

At Cononley Primary School:

- web filtering is provided by Smoothwall.
- changes can be made by NYES Digital.
- overall responsibility is held by the DSL Catherine Pickles
- technical support and advice, setup and configuration are from NYES Digital
- regular checks are made at least termly, by Catherine Pickles (DSL) and Rachel Price Wait, Filtering and Monitoring Governor, to ensure filtering is still active and functioning everywhere. These are carried out using the filtering and monitoring tool on the SWGFL site and the resulting notifications from Smoothwall are kept in the DSL's email folder.
- an annual review is carried out as part of the online safety audit to ensure a whole school approach.

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

At Cononley Primary School, the internet connection is provided by NYES Digital. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

security, including a web filtering system called Smoothwall, a cloud filter and cloud safeguarding platform.

**How Smoothwall protects against Ofsted's online safety guidelines**

- Oversee safe use of technology**  
With Smoothwall, you can rest assured that you are providing enterprise-level protection for your school, allowing your children to learn in a safe environment and use the internet as an aid to academic development.
- Keep children and learners safe**  
Our real-time content aware web filter ensures that any unwanted content on the internet is kept out of reach for children. With the addition of our firewall, you can also ensure you are protected from external threats.
- Flexible, age-appropriate e-Safety policy**  
Smoothwall allows you to easily build filtering policies based on the user or group. This means that administrators or delegated teaching staff can allow access for certain sites or apps for different groups of people.
- Incidents are reported and monitored**  
Using our new safeguarding reports feature, you are able to monitor blocked actions and search terms, allowing you to identify any safeguarding concerns and report on it, keeping a full log of any incidents.

**smoothwall**  
The Web You Want

## Messaging/commenting systems (incl. email, learning platforms & more)

### Authorised systems

- Staff at this school use NYES digital email system for all school emails; this system is managed by NYES Digital on the school's behalf. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection
- In addition to NYES digital email system, the comms system on the school MIS, Scholarpack, is also used by the school office and Headteacher to send emails and texts to parents / carers and staff. Parents / carers cannot respond to emails / texts sent from the school MIS comms.
- Pupils at Cononley Primary School do not have school email addresses; however, they can use Purple Mash Email (internal email system on the cloud based learning platform). Emails can only be sent to other pupils or teachers in school. Pupils are not allowed to send messages that are rude or offensive. This is monitored by the class teacher and Computing lead and transgression will be dealt with through the school Behaviour Policy.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

General principles for email use are as follows:

- Email (NYES digital system) and emails and texts (Scholarpack MIS comms system) are the only means of electronic communication to be used between staff and parents.
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff

See also the social media section of this policy.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

## Behaviour / usage principles

- More detail for all the points below are given in the [Social media](#) section of this policy as well as the school's acceptable use policies, behaviour policy and staff code of conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Information Policy and Privacy Notices and only using the authorised systems mentioned above. (See website for policies: <https://www.cononleyprimary.org.uk/key-info/school-policies> )
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language,

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

## Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Cononley Primary School has a clear Information Security and Information Policy and Privacy notices which staff, governors and volunteers must follow at all times. (See website- <https://www.cononleyprimary.org.uk/key-info/school-policies>)

## School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the Headteacher.

The site is hosted by Great School Websites

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected.

## Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents/Carers are asked to give permission for their child's photograph to be taken and used for the reasons listed below. (Children's names will NOT be published with the photograph.)

- Weekly Bulletin
- Half Term Newsletter
- Cononley Primary School website
- Press release
- Twitter Account
- Tapestry (EYFS Online Journal)

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

All staff are governed by their contract of employment and the school's Acceptable Use Policy. Volunteers are also required to follow the school Acceptable Use Policy.

-At Cononley Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

-Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

-Staff and parents are reminded about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

-We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.

-Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

-Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they or a friend are subject to bullying or abuse.

## Social media

### Our SM presence

Cononley Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk)) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner even there are no official/active school social media accounts.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies and online rules (for pupils) we expect everybody to behave in a positive manner, engaging respectfully on social media, in the same way as they would face to face. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

On occasions some parents are tempted to make comments about the school, school staff, other parents and/or pupils on social media. Social media is not the forum for raising concerns or complaints about the school. If parents have a concern about the school, they can raise their concern directly with the Headteacher and complaints can be raised through the school's Complaints Procedure.

Parents and carers should take care when posting messages on social media. Parents are expected to treat everyone with respect and professionalism – even on social media - and adults should set a good example to their children and other pupils. Do not use social media to criticise the school or its staff or pupils or make inappropriate comments.

In the event that any pupil or parent/carer of a pupil is found to be posting inappropriate comments on social media, they will be reported to the appropriate 'report abuse' section of the social media site and consideration will be given to taking further action. Making potentially defamatory, offensive or derogatory comments about others on social media could have legal implications. In addition, threats of violence can lead to a criminal action. The school will also expect any pupil or parent/carer to remove such inappropriate comments immediately.

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email is the official electronic communication channel between parents and the school.

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.

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

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

**\*\* Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the Headteacher (also Designated Safeguarding Lead).**

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 6 years, there have been 333 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/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 the use of images (see school privacy agreements) and permission is sought before uploading photographs, videos or any other information about other people.

## Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

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

Cononley Primary School has a clear policy on the use of mobile and smart technology, including smart watches (see also Child Protection Policy).

- Children are not allowed 'Fit Bits' (or similar devices) or Smart Watches in school. Children are not allowed mobile phones in school unless there are exceptional circumstances. Parents/ carers should seek permission from the headteacher and class teacher via email if there is a reason why their child needs to bring a mobile phone to school. If permission is granted, it is on the understanding that the phone will be handed to the class teacher at the start of the day and returned at the end of the school day. All such devices must be switched off until the end of the day. Under no circumstance should pupils use their personal mobile devices/phones to take images of any other pupil or any member of staff.
- The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas (the school office and staffroom) during school hours.
- **EYFS staff** must keep their mobile phones locked in a cabinet outside the EYFS classroom

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- 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. 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 and turned off when they are on site. When at school events, parents / carers may take photographs and videos of their own child/ren but these images are for private use and must not be shared on social media.

## Use of school devices

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas (staffroom or school office) during school hours. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices.
- **Parents** have no access to the school network or wireless internet on personal devices.
- **Trips / events away from school** Teachers may need to take their personal phone in case of emergency. They must 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 '[Searching, screening and confiscation: advice for schools](#)', 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. Please see the 'Prohibited Items' section of the Behaviour Policy.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## 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 Child Protection Policy, the Staff Code of Conduct and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach: <https://www.cononleyprimary.org.uk/key-info/safeguarding>

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2023) 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 overblocking, gaps in provision or pupils bypassing protections.

## Headteacher – Catherine Pickles

### Key responsibilities:

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school).
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL—in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
  - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements

## Designated Safeguarding Lead / Online Safety Lead – Catherine Pickles

**Key responsibilities** (remember the DSL can delegate certain online-safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- The DSL should “take **lead responsibility** for safeguarding and child protection (including **online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure “An effective whole school approach to online safety as per KCSIE
- In 2023/4 working to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home. [ [LGfL’s Safeguarding Shorts: Filtering for DSLs and SLT](#) twilight provides a quick overview and there is lots of information for DSLs at [safefiltering.lgfl.net](#) and [appropriate.lgfl.net](#) ]
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL’s clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
  - In 2023/4 this must include filtering and monitoring and help them to understand their roles
  - all staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at [kcsietranslate.lgfl.net](#) (B the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
  - cascade knowledge of risks and opportunities throughout the organisation
  - [safecpd.lgfl.net](#) has helpful CPD materials including PowerPoints, videos and more
- Ensure that ALL governors and trustees undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated –[ LGfL’s Safeguarding Training for school governors is free to all governors at [safetraining.lgfl.net](#) ]
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language [ see [spotlight.lgfl.net](#) for a resource to use with staff on how framing things linguistically can have a safeguarding impact, and some expressions we use might be unhelpful ]
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school) – [see LGfL’s template with questions to use at [onlinesafetyaudit.lgfl.net](#) ]

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and “undertake Prevent awareness training.” – see [safetraining.lgfl.net](https://safetraining.lgfl.net) and [prevent.lgfl.net](https://prevent.lgfl.net)
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends – see [safeblog.lgfl.net](https://safeblog.lgfl.net) for examples or sign up to the [LGfL safeguarding newsletter](#)
- Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework ‘[Education for a Connected World – 2020 edition](#)’) and beyond, in wider school life
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents – dedicated resources at [parentsafe.lgfl.net](https://parentsafe.lgfl.net)
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine, e.g. a [survey to facilitate disclosures](#) and an online form on the school home page about ‘something that worrying me’ that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don’t dismiss it as banter (including bullying).
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, [template you can use at [safepolicies.lgfl.net](https://safepolicies.lgfl.net) with provisions] and those hired by parents. [ share [the Online Tutors – Keeping Children Safe](#) poster at [parentsafe.lgfl.net](https://parentsafe.lgfl.net) to remind parents of key safeguarding principles ]

**Governing Body, led by Safeguarding Link Governor – Katie Mason, and Filtering and Monitoring Governor, Rachel Price Waite.**

**Key responsibilities (quotes are taken from Keeping Children Safe in Education)**

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#)
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated – [ LGfL’s Safeguarding Training for school governors is free to all governors at [safetraining.lgfl.net](#) ]
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards [ there is guidance for governors at [safefiltering.lgfl.net](#) ]
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology

**PSHE / RSHE Lead – Jaki Fraser**

## Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. “This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils’ lives.” [ training is available at [safetraining.lgfl.net](#) ]

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#) in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress” – [ see LGfL’s SafeSkills Online Safety Quiz and diagnostic teaching tool at [safeskillsinfo.lgfl.net](https://safeskillsinfo.lgfl.net) ] to complement the computing curriculum,.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

## Computing Lead – Ross Milner

### Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

## Subject / aspect leaders

### Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- Ensure subject specific action plans also have an online-safety element

## Network Manager/other technical support roles – NYES Digital / LA Safeguarding Officer

### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. [ LGfL has a free template you can use at <https://onlinesafetyaudit.lgfl.net> ] This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, [ we recommend you signpost them to [LGfL's Safeguarding Shorts: Filtering for DSLs and SLT](#) twilight at [safetraining.lgfl.net](https://safetraining.lgfl.net) which provides a quick overview to help build their understanding ] protections for pupils in the home [e.g. LGfL HomeProtect filtering for the home – <https://homeprotect.lgfl.net> ] and remote-learning. [ see [remotesafe.lgfl.net](https://remotesafe.lgfl.net) for guidance ]
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable Monitor the use of school technology, online platforms and social media presence.

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

- and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements [ see website audit tool at [websitesiterag.lgfl.net](https://websitesiterag.lgfl.net) / this may well be part of someone else's role, but the technical team is likely to play at least some role in working with the web team – move this bullet point as appropriate ]

## Data Protection Officer (DPO) – Veritau

### Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at [safepolicies.lgfl.net](https://safepolicies.lgfl.net), but you should check the rules in your area.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

## Volunteers

### Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications

# Cononley Primary School Online Safety Policy - 2023/4 DRAFT

## Pupils

### Key responsibilities:

Read, understand, sign and adhere to the student/pupil acceptable use policy

## Parents/carers

### Key responsibilities:

- Read, and adhere to the school's parental acceptable use policy (AUP), read the pupil Internet Safety Rules and encourage their children to follow these rules.

## External groups including parent associations –Friends of Cononley School

### Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers