


Introduction

Key people / dates

| | | |
|--|---|---|
|  <small>CONONLEY PRIMARY SCHOOL Inspiring and Challenging Our Children</small> | Designated Safeguarding Lead (DSL) team | Catherine Pickles (DSL) Jaki Fraser (Deputy DSL) |
| | Online-safety lead | Catherine Pickles (DSL) |
| | Link governor for safeguarding (includes online safety) | Katie Mason |
| | PSHE/RSHE/RSE lead | Jaki Fraser |
| | Network manager / other technical support | NYES Digital Technician: Steve Bunce |
| | Date this policy was reviewed and by whom | Full Governing Body |
| | Date of next review and by whom | March 2024 (FGB) |

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’ 2022 (KCSIE), ‘Teaching Online Safety in Schools’ 2019, statutory RSHE guidance 2019 and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside your school’s statutory 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. We recommend you read the guidance at safepolicies.lgfl.net before reissuing your school policies for online safety, safeguarding and AUPs to see what needs changing. Although many aspects will be informed by legislation and regulations, you should involve staff, governors, pupils and parents in writing and reviewing the policy (KCSIE stresses making use of teachers’ day-to-day experience on the ground). 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 2022/2023?

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022). These areas provide a helpful approach to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all three. This is evident in Ofcom’s Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something ‘worrying or nasty’ online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other apps and sites.

KCSIE 2022 highlights additional risks e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families, including sexual and criminal exploitation, serious youth violence, upskirting and sticky design.

Analysis from the Centre of Expertise on Child Sexual Abuse also highlights the prevalence of child sexual abuse, with 500,000 children estimated to experience child sexual abuse every year, whilst the Internet Watch Foundation has identified the growing risk of children, especially girls aged 11-13, targeted online by sex predators, with a three-fold increase in abuse imagery of 7–10-year-olds. This highlights transition years as crucial in the fight against sexual exploitation, in primary and secondary. See [cse.lgfl.net](https://www.cse.lgfl.net) for resources to support DSLs, RSHE/PSHE leads and parents, including the [Undressed](#) campaign.

Following the Ofsted review into **peer-on-peer sexual abuse**, schools should follow the updated advice on sexual violence and harassment guidance (note this is no longer a standalone document and now incorporated in Part 5 of KCSIE where the term ‘peer-on-peer’ has been replaced with ‘child-on-child’) which has many online implications. Schools will need to review their policies and practice to reference these updates and ensure appropriate processes are in place to allow pupils to report sexual harassment and abuse concerns freely, knowing these will be taken seriously and dealt with swiftly and appropriately – ensure pupils are aware of the new [NSPCC helpline](#) and your school’s internal reporting channels. Ways we can help you stay up to date with the latest news, risks, opportunities, best-practice and trends include the LGfL DigiSafe [blog](#), [newsletter](#) and our [Twitter](#)/[Facebook](#) channels.

Following covid, it is important to remember more time spent online increases the risk for grooming and exploitation (CSE, CCE and radicalisation) and potentially reduces opportunities to disclose such abuse. The quick survey at safeposters.lgfl.net may help to surface some of these issues. Teachers may also find LGfL’s SafeSkills Online Safety Quiz and diagnostic teaching tool at safeskillsinfo.lgfl.net particularly useful to capture and assess pupil resilience and competence for digital life, as recommended by KCSIE.

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

| | |
|--|-------------------------------------|
| What’s different about this policy for September 2022? | Error! Bookmark not defined. |
| Introduction | 1 |
| Key people / dates | 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 2022/2023? | 2 |
| How will this policy be communicated? | 3 |
| Contents | 3 |
| Overview | 6 |
| Aims | 6 |
| Further Help and Support | 6 |
| Roles and responsibilities | 7 |
| Education and curriculum | 7 |

| | |
|---|----|
| | 8 |
| Actions where there are concerns about a child | 10 |
| Sexting – sharing nudes and semi-nudes | 12 |
| Upskirting | 13 |
| Bullying | 13 |
| Sexual violence and harassment | 13 |
| Misuse of school technology (devices, systems, networks or platforms) | 13 |
| Social media incidents | 14 |
| Data protection and data security | 15 |
| Appropriate filtering and monitoring | 15 |
| Email | 16 |
| School website | 17 |
| Cloud platforms | 17 |
| Digital images and video | 18 |
| Social media | 19 |
| Cononley Primary School’s SM presence | 19 |
| Staff, pupils’ and parents’ SM presence | 19 |
| Device usage | 21 |
| Personal Devices | 21 |
| Network / internet access on school devices | 22 |
| Appendix 1 – Roles | 23 |
| All staff | 24 |
| Headteacher– Catherine Pickles | 25 |
| Designated Safeguarding Lead / Online Safety Lead – Catherine Pickles | 26 |
| Governing Body, led by Safeguarding Link Governor, Katie Mason | 28 |
| PSHE / RSE Lead Jaki Fraser | 29 |
| Computing Lead – Ross Milner | 30 |
| Subject leaders | 30 |
| Network Manager/technician – NYES Digital | 31 |
| Data Protection Officer (DPO) – Veritau | 31 |
| Volunteers | 32 |
| Pupils | 32 |
| Parents/carers | 32 |



Cononley Primary School

External groups including parent associations – FoCS Friends of Cononley School 33

Appendix 2 – Related Policies and Documents 34

Aims

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

- Setting out expectations for all Cononley 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 filtering and monitoring through effective collaboration and communication with technical colleagues
- 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 our Cononley Primary School Child Protection Policy. The Headteacher /DSL Catherine Pickles will handle referrals to local authority multi-agency safeguarding teams (MAST) and the Headteacher Catherine Pickles (also DSL) will handle referrals to the LA designated officer (LADO). The local authority and third-party support organisations you work with, such as the NSPCC, may also have advisors to offer general support.

Our school website 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

Scope

This policy applies to all members of the Cononley Primary School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, 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.

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

RSE/PSHE 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.” At Cononley Primary School, we use simple quizzes and surveys such as LGfL’s SafeSkills Online Safety Quiz and diagnostic teaching tool which is linked to statements from UKCIS Education for a Connected

World framework, enabling teachers to monitor progress throughout the year and drill down to school, class and pupil level to identify areas for development at safeskillsinfo.lgfl.net]

The following curriculum subjects have the clearest online safety links:

- Relationships and Sex Education (RSE) and Personal, Social, Health and Economic Education(PSHE)
- Computing

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 subject leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, new technology etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils 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 2022)

At Cononley Primary School, we use Smoothwall to filter and monitor online activity. NYES Digital provide technical support to ensure that Smoothwall runs effectively.

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.

The DSL regularly checks the resources available at saferesources.lgfl.net (updated theme-based resources, materials and signposting for teachers and parents) and shares them with staff at Safeguarding Briefings and other Staff Training, and with Parents / carers via the safeguarding information in the Weekly Bulletin.

At Cononley Primary School, we recognise the importance of online safety and broader digital resilience; our Computing scheme (Purple Mash) and PSHE / RSE scheme (Kapow) incorporate the framework ‘Education for a Connected World – 2020 edition’ from UKCIS (the UK Council for Internet Safety).

Handling online-safety 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/RSE).

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 (including 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 online safety, 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 designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, 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:

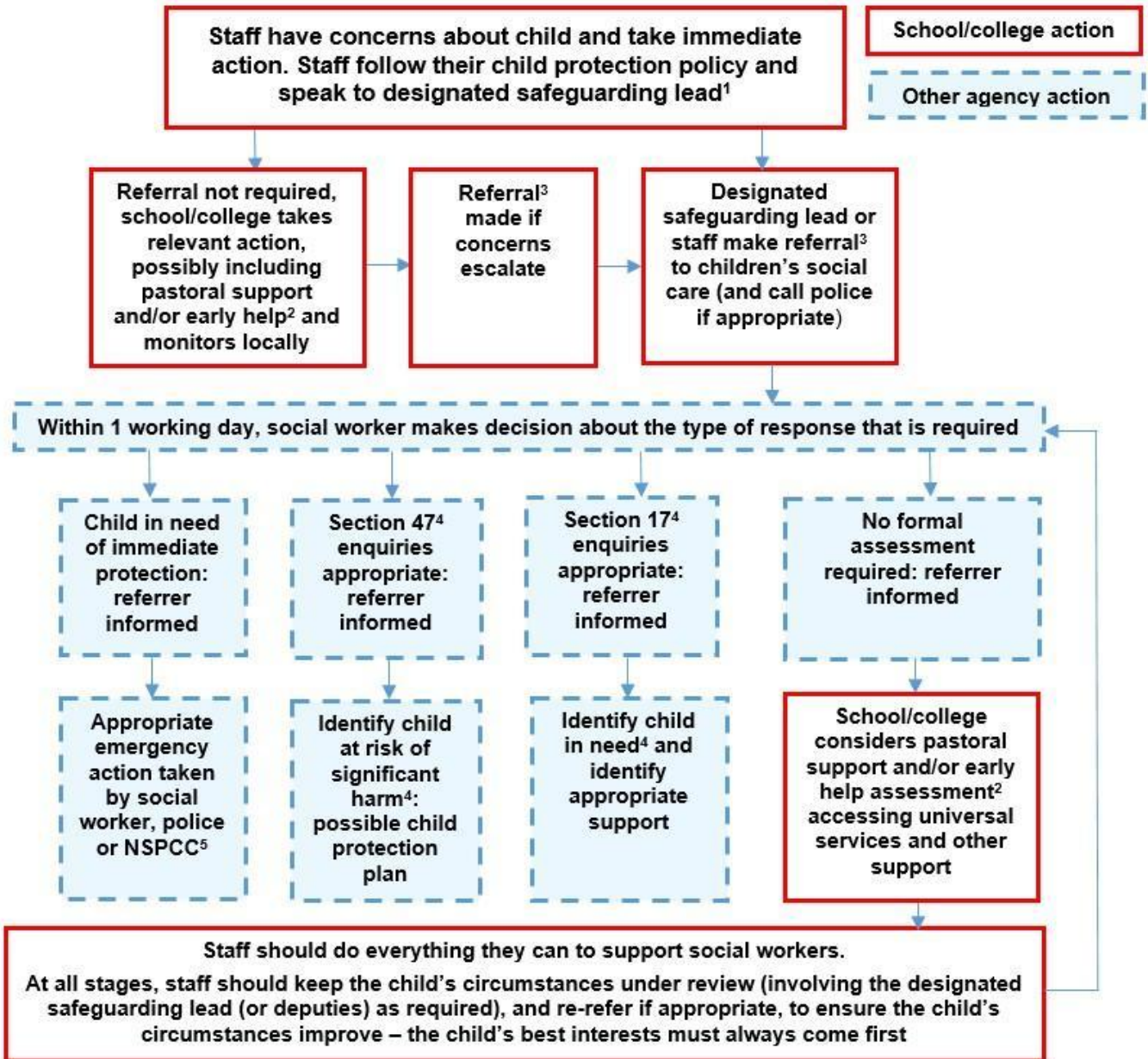
0800 028 0285

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 new DfE guidance [Behaviour in Schools, advice for headteachers and school staff](#) July 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 disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

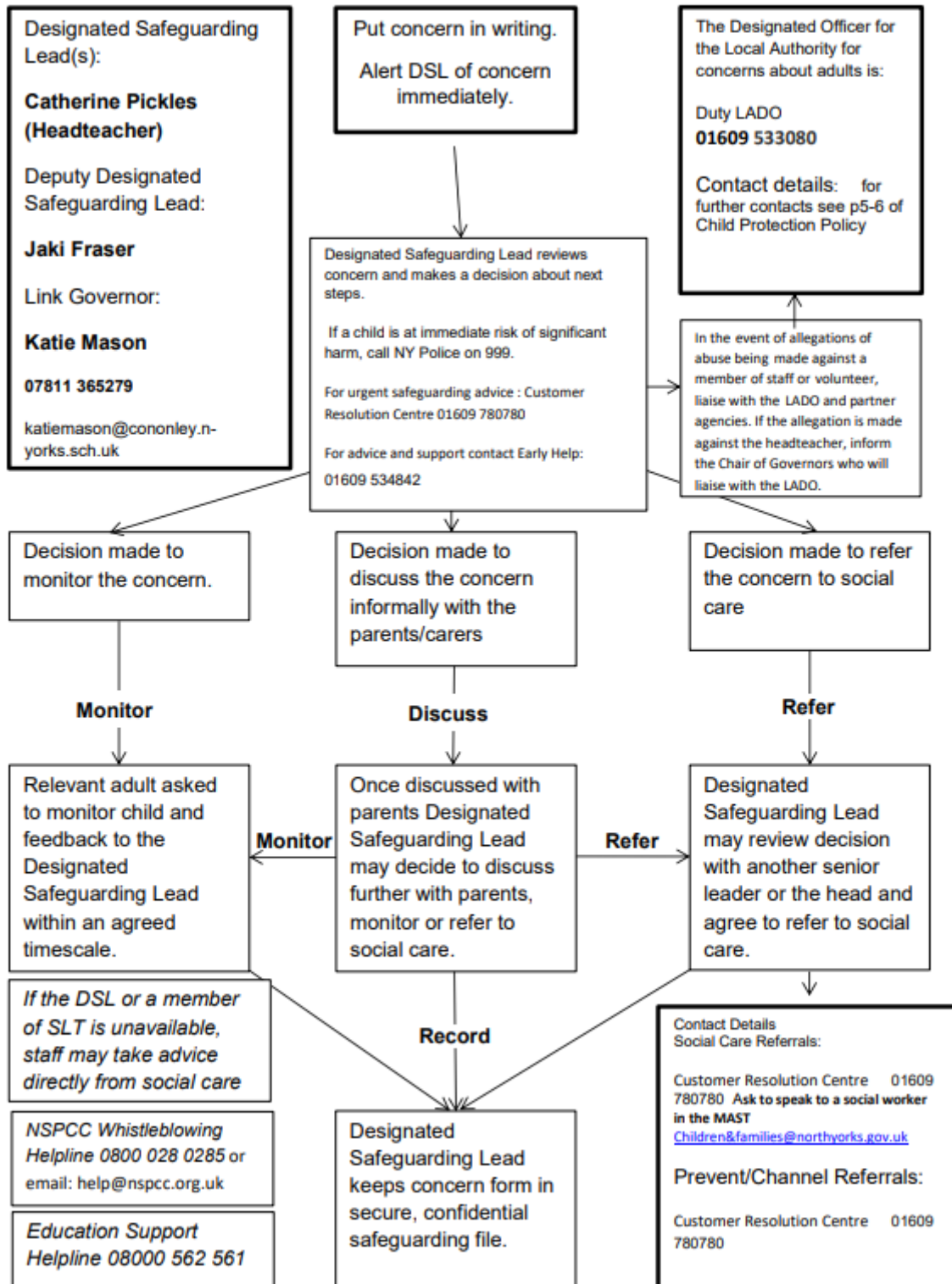
Actions where there are concerns about a child

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 Flow Chart for Raising Safeguarding Concerns

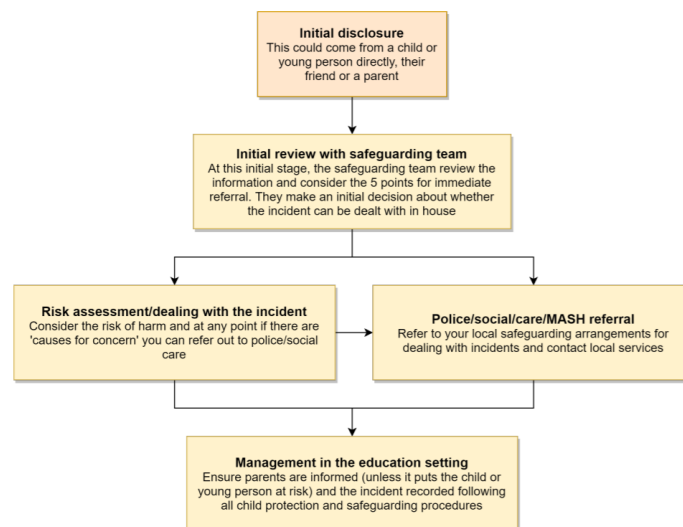
FLOW CHART FOR RAISING SAFEGUARDING CONCERNS ABOUT A CHILD- always refer to the Cononley Primary School Child Protection Policy.



When dealing with cases of sexting (sharing nudes and semi nudes) staff at Cononley Primary School will refer to the updated 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

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>

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

DfE guidance on sexual violence and harassment has now been incorporated into Keeping Children Safe in Education and is no longer a document in its own right. It would be useful for all staff to be aware of this updated guidance: Part 5 covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL 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.

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 our Acceptable Use Policies 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.

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.

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 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 data security

GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net; there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

“GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced ‘safeguarding’ as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.**”

All pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements, which can be found on our school website:

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

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: Sophos Anti-Virus, Egress, Smoothwall.

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. Whenever possible, Egress is used to encrypt all non-internal emails sharing pupil data.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At this 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 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

Email

- 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.

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.

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 to the Headteacher. The site is hosted by Great School Websites.

The DfE has determined information which must be available on a school website

Where other staff submit information for the website, they are asked to remember:

- 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.
- Where pupil work, images or videos are published on the website, their identities are protected and names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

Senior leader and governors know the importance of considering data protection before adopting a cloud platform or service – see the school website for our Information Policy: <https://www.cononleyprimary.org.uk/key-info/school-policies>

For online safety, basic rules of good password hygiene (“Treat your password like your toothbrush –never share it with anyone!”), expert administration and training can help to keep staff and pupils safe, and to avoid incidents.

The following principles apply:

- Privacy statements inform parents and when and what sort of data is stored in the cloud
- The DPO advises on new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil/student 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

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 annually 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

Cononley Primary School's 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) 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.

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).

** 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 Digital Images and Video (see page) and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal Devices

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.
 - 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.

Network / internet access on 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.

Please read the relevant roles & responsibilities section from the following pages.

School staff – note that you may need to read two sections – if your role is reflected here, you should still read the “All Staff” section.

Roles:

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

Key responsibilities:

- Read and follow this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures
- Know that the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) is Catherine Pickles (Headteacher); notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Sign and follow the staff acceptable use policy and code of conduct.
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE / RSE curriculum, both outside the classroom and within the curriculum, supporting 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 in school or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites.
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils to follow the online safety rules at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know.
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues

- Model safe, responsible and professional behaviours in your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this [Online Reputation](#) guidance for schools.

Headteacher– Catherine Pickles

Key responsibilities:

- 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 [LGfL's Safeguarding Training for School Governors is free to all governors at safetraining.lgfl.net]
- 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. At Cononley Primary School, we use NYES Digital to provide and support our filtering and monitoring and email systems.
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – in particular understand what is blocked or allowed for whom, when, and how. Note that KCSIE 2022 strengthens the wording for this. [[LGfL's Safeguarding Shorts: Filtering for DSLs and SLT](#) twilight provides an overview]
- 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 [see remotesafe.lgfl.net for policy guidance and an infographic overview of safeguarding considerations for remote teaching technology]
- Assign responsibility to a nominated member of staff to carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process (this new addition has come into KCSIE 2022 for the first time)

- 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 GDPR-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 [websitesafe.lgfl.net can help you with this]

Designated Safeguarding Lead / Online Safety Lead – Catherine Pickles

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

- “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] ... this **lead responsibility** should not be delegated”
- Work with technical staff from NYES digital to review protections for **remote-learning** procedures, rules and safeguards [there is guidance at remotesafe.lgfl.net]
- Ensure “An effective whole school approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated

- Liaise with the Headteacher and Chair of Governors to 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 online safety 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 staff and technical colleagues at NYES Digital 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]
- Work with the headteacher, DPO and governors to ensure a GDPR-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 and 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. At Cononley Primary School the DSL accesses Safeguarding Pro, NYSCP bulletin, NYCC HR Bulletin and NYES Digital Bulletin. Other useful resources include safeblog.lgfl.net.
- Ensure that online safety education is embedded across the curriculum in line with the statutory PSHE / RSE guidance (e.g. by use of the updated UKCIS framework ‘[Education for a Connected World – 2020 edition](https://www.ukciscis.org/education-for-a-connected-world-2020-edition)’) and beyond, in wider school life. At Cononley, our Computing Curriculum (Purple Mash) and our PSHE Curriculum (Kapow) both incorporate this framework.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents – there are dedicated resources at parentsafe.lgfl.net. There is a safeguarding information section in our weekly bulletin, which often refers to online safety, and there is a section of our school website with links to online safety information:
<https://www.cononleyprimary.org.uk/parents/line-safety-and-safeguarding-information>
- Communicate regularly with DSL and the safeguarding governor 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/lockdown, e.g. a reminder to tell parents/carers.
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this). Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why. Also, as per KCSIE “be careful that ‘over blocking’ does not lead to unreasonable restrictions”. [\[LGfL’s Safeguarding Shorts: Filtering for DSLs and SLT](#) twilight provides a quick overview.
- Ensure KCSIE ‘Part 5: Sexual Violence & Sexual Harassment’ is understood and followed throughout the school and that 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).
- Facilitate training and advice for all staff, including supply teachers:
 - 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
 - Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
 - cascade knowledge of risks and opportunities throughout the organisation
 - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- 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 with provisions] and those hired by parents. [share [the Online Tutors – Keeping Children Safe](#) poster at parentsafe.lgfl.net to remind parents of key safeguarding principles]
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Governing Body, led by Safeguarding Link Governor, Katie Mason

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

- 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
- “Ensure appropriate filters and appropriate monitoring systems are in place [but...] be careful that ‘overblocking’ does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding”.
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards [see remotesafe.lgfl.net for guidance]
- “Ensure an appropriate **senior member** of staff, from the school **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support...”
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised. At Cononley, the online safety coordinator is the Headteacher / DSL.
- Work with the DPO, DSL / headteacher to ensure a GDPR-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; and all working directly with children have read Annex B
- “Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated in line with advice from the local three safeguarding partner integrated, aligned and considered as part of the overarching safeguarding approach.” There is further support for this at cpd.lgfl.net
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology.”
-

PSHE / RSE Lead Jaki Fraser

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / relationships and sex education (RSE) 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."

- 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]
- This complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSE.
- Note that an RSE 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 RSE 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 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 RSE 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
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – NYES Digital

Key responsibilities:

- 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.

Data Protection Officer (DPO) – Veritau

Key responsibilities:

- NB – this document is not for general data-protection guidance;
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule 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, but you should check the rules in your area.

- Work with the DSL / headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- 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 / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the school online safety rules
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read and promote the school's parental acceptable use policy (AUP) and read the pupil online safety rules and encourage their children to follow it
- Talk to the school if they have any concerns about their children's and others' use of technology

- Promote positive online safety and 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.
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the [Online Tutors – Guidance for Parents and Carers](#) poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

External groups including parent associations – FoCS 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

Appendix 2 – Related Policies and Documents

For related documents and policies marked * the latest version or a template we will use is available at safepolicies.lgfl.net

1. Child Protection log and Safeguarding log (CPOMS)
2. Child Protection
3. Behaviour Policy / Anti-Bullying Policy
4. Staff Code of Conduct / Handbook
5. *Acceptable Use Policies (AUPs) for:
 - *Pupils (On-line safety Rules)
 - *Staff, Volunteers Governors & Contractors
 - *Parents
6. *Prevent Risk Assessment Template
7. *Online-Safety Questions from the Governing Board (UKCIS)
8. *Education for a Connected World cross-curricular digital resilience framework (UKCIS)
9. *Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
10. *Working together to safeguard children (DfE)
11. *Searching, screening and confiscation advice (DfE)
12. *Sharing nudes and semi-nudes guidance from UKCIS:
 - *How to respond to an incident - overview for all staff
 - *Full guidance for school DSLs
 - *Online Safety Audit for Trainee (ITT) & Newly Qualified Teachers (NQT)
13. *Prevent Duty Guidance for Schools (DfE and Home Office documents)
14. *Cyber security advice, procedures etc
15. *Preventing and tackling bullying (DfE)
16. Cyber bullying: advice for headteachers and school staff (DfE) – find this at bullying.lgfl.net
17. *RAG (red-amber-green) audits for statutory requirements of school websites