Coopers Lane Primary School

Online Safety Policy

Author/ Checked:	Amy Riley/Paul Hooper	Date: Summer 2024
Reviewed/ Approved by:	Governing Body	Date: Summer 2024
Issue date:	Summer 2024	Next Review due by: Summer 2025

A Coopers Lane Learner...

...is inspired to be the best version of themselves and takes pride in all they do.

Responsibility

Honesty

...has the tools needed to be confident in making positive choices about behaviour and learning.

Kindness

...has empathy towards others and values the opinion of everyone.

...is excited to share their fun, relevant and memorable learning experiences with family & friends.

all different • all equal • all smiling • COOPERS LANE

...understands the importance of not giving up, embracing challenge and seeking help when needed.

...is a fabulous role model and a respectful citizen, embracing and celebrating the rich, diverse community in which they live.

Respect

Happiness

Love

...develops a curiosity and wonder of the wider world around them.

Perseverance

Contents

1. Aims

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

- Setting out expectations for all Coopers Lane Primary 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)

This policy applies to all members of the community (including teaching and support staff, supply teachers, 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.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study, Relationships, health and Sex Education Policy and the Computing curriculum.

3. Main online safety risks

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see KCSIE). 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 aps and sites.

KCSIE 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 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.

4. Roles and responsibilities

4.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governor who is responsible for safeguarding will oversee online safety.
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

4.2 The headteacher
The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The designated safeguarding lead
Details of the school's designated safeguarding lead (DSL) and deputies are set out in our safeguarding policy.
The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
This list is not intended to be exhaustive.

4.4 The ICT technician
The ICT technician is responsible for:
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported to the DSL
- This list is not intended to be exhaustive.

4.5 All staff and volunteers
All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- This list is not intended to be exhaustive.

4.6 Parents

Parents are expected to:
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

4.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

5. Educating pupils about online safety

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.

Our teaching focuses on underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app.

The following subjects have the clearest online safety links

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)

- Computing

However, 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.

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.

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Pupils in **Key Stage 2** will be taught to:
- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5a. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings where relevant.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. 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/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 online-safety lead / designated safeguarding lead 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 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):

- Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)

Coopers Lane Primary 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 online safety lead / 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).

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.

7. Cyber-bullying

7.1 Definition
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy, cyber bullying policy and anti-bullying policy.)

7.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy and cyber bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:
● Cause harm, and/or
● Disrupt teaching, and/or
● Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
● Delete that material, or
● Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
● Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 - 5). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 - 5.

9. 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 LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:
1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Coopers Lane Primary we have decided that option 3 is appropriate because it monitors to a higher level. London Grid for Learning provides a technology-based monitoring system that actively monitors use through keywords and other indicators across devices. This system is particularly effective at drawing attention to concerning behaviours, communications or access.

10. Pupils using mobile devices in school

Pupils in Year 5 and Year 6 may bring mobile devices into school, but are not permitted to use them during:
● Lessons
● Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Mobile phones must be handed in to the school office at the start of the day and collected at the end of the day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

11. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of

their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

Work devices must be used solely for work activities.

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Staff, pupils' and parents' social media 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 which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other 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.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

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. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

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). You may wish to refer to the new Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

The school has an official Twitter and Instagram account (managed by the Senior Leadership Team) and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children or staff. Any posts or comments that identify children or staff will be removed.

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

Pupils/students 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.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, 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 DSL (if by a child) or to the Headteacher (if by a staff member).
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.
The statements of the Acceptable Use Policies (Appendices 1-5) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Please also see our Social Media Policy.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). They will also complete a training needs audit as required (appendix 6).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

15. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using My Concern.

This policy will be reviewed annually by the school safeguarding team. At every review, the policy will be shared with the governing board.

16. Links with other policies

This online safety policy is linked to our:
- Safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Cyber-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Social Media

Appendix 1: acceptable use agreement KS1 pupils

LGfL **DigiSafe**
keeping children safe

Acceptable Use Policy (AUP) for
KS1 PUPILS

My name is _____
⊞

To stay **SAFE online and on my devices**:	✓
1. I only **USE** devices or apps, sites or games if a trusted adult says so	
2. I **ASK** for help if I'm stuck or not sure	
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I look out for my **FRIENDS** and tell someone if they need help	
6. I **KNOW** people online aren't always who they say they are	
7. Anything I do online can be shared and might stay online **FOREVER**	
8. I don't keep ~~SECRETS~~ or do **DARES AND CHALLENGES** just because someone tells me I have to	
9. I don't change **CLOTHES** or get undressed in front of a camera	
10. I always check before **SHARING** personal information	
11. I am **KIND** and polite to everyone	

My trusted adults are:

_____ **at school**

_____

_____ **at home**

_____

Appendix 2: acceptable use agreement KS2 pupils

LGfL DigiSafe *keeping children safe*

Acceptable Use Policy (AUP) for
KS2 PUPILS

These statements can keep me and others safe & happy at school and home

1. *I learn online* – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.

2. *I behave the same way on devices as face to face in the classroom, and so do my teachers* – If I get asked to do anything that I would find strange in school, I will tell another teacher.

3. *I ask permission* – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.

4. *I am creative online* – As well as looking at things from other people on apps, sites and games, I also get creative to learn and make things, and I remember my Digital 5 A Day.

5. *I am a friend online* – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.

6. *I am not a bully* – I know just calling something banter doesn't make it ok as it could become bullying. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

7. *I am a secure online learner* – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

8. *I am careful what I click on* – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.

9. *I ask for help if I am scared or worried* – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.

10. *I know it's not my fault if I see or someone sends me something bad* – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

11. *I communicate and collaborate online* – with people I already know and have met in real life or that a trusted adult knows about.

12. *I know new online friends might not be who they say they are* – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

13. *I check with a parent/carer before I meet an online friend* the first time; I never go alone.

14. *I don't do live videos (livestreams) on my own* – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

15. *I keep my body to myself online* – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

DigiSafe LGfL
keeping children safe

Acceptable Use Policy (AUP) for
KS2 PUPILS

16. *I say no online if I need to* – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

17. *I tell my parents/carers what I do online* – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

18. *I follow age rules* – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.

19. *I am private online* – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

20. *I am careful what I share and protect my online reputation* – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

21. *I am a rule-follower online* – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.

22. *I am part of a community* – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

23. *I respect people's work* – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

24. *I am a researcher online* – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes

_____

Outside school, my trusted adults are

_____

I know I can also get in touch with Childline

Signed: _____   **Date:** _____

Appendix 3: acceptable use agreement parents

LGfL **DigiSafe** *keeping children safe*   **Acceptable Use Policy (AUP) for PARENTS**

Background

We ask all children, young people and adults involved in the life of Coopers Lane Primary to sign an Acceptable Use Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an Acceptable Use Policy.

We tell your children that **they should not behave any differently when they are out of school or using their own device or home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

What am I agreeing to?

1. I understand that Coopers Lane Primary uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, including during any remote learning periods.

4. I will promote positive online safety and model safe, responsible and positive behaviours in my 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.

5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.

6. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.

7. I understand that for my child to grow up safe online, they will need positive input from school and home, so I will talk to my child about online safety and can refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life

LGfL DigiSafe *keeping children safe*

Acceptable Use Policy (AUP) for PARENTS

online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc...

8. I understand that my child needs a safe and appropriate place to do home learning.
9. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
10. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
11. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which they have signed, and I understand that they will be subject to sanctions if they do not follow these rules.
12. I can find out more about online safety at Coopers Lane Primary by reading the full Online Safety Policy and can talk to the head teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

~~~~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____

Date: _____

Appendix 4: acceptable use agreement staff, governors, volunteers and visitors

LGfL DigiSafe *keeping children safe*

Acceptable Use Policy (AUP) for STAFF, GOVERNORS, VOLUNTEERS

What is an AUP?

We ask all children, young people and adults involved in the life of Coopers Lane Primary to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Coopers Lane Primary's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc

If you have any questions about this AUP or our approach to online safety, please speak to a member of the Senior Leadership Team.

What am I agreeing to?

1. (This point for staff and governors): I have read and understood Coopers Lane Primary's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult).
3. I will follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
4. I will 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 - and maintain an attitude of 'it could happen here'
5. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language

DigiSafe LGfL
keeping children safe

Acceptable Use Policy (AUP) for
STAFF, GOVERNORS, VOLUNTEERS

6. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the RSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.

7. During remote learning:
   o I will not behave any differently towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
   o I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
   o I will not take secret recordings or screenshots of myself or pupils during live lessons.
   o I will conduct any video lessons in a professional environment as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
   o I will log and report any issues for live lessons immediately to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult) if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students

8. I understand that in any periods of home learning, school closures or potential lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

9. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

10. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
    • not sharing other's images or details without permission
    • refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

11. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.

12. I will not capture general digital images/video on my personal devices. If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL.

13. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either.

14. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access,

LGfL DigiSafe
keeping children safe

Acceptable Use Policy (AUP) for
STAFF, GOVERNORS, VOLUNTEERS

attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify a member of the Senior Leadership Team if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

15. I will not store school-related data on personal devices, storage or cloud platforms. USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

16. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

17. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.

18. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

19. I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: _____

Name: _____

Role: _____

Date: _____

Appendix 5: acceptable use agreement social stories

What I Must do to Keep Safe Online and With Devices

Online means anything connected to the internet. Most devices and apps are connected to the internet.
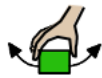
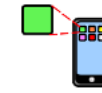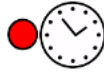Devices are technology like: computers, laptops, games consoles, tablets and smart phones.
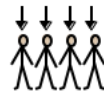
Acceptable Use Policy

I will only use the devices I am allowed to use.

I will ask a trusted adult before I use new websites, games or apps.

I will ask for help if I'm stuck or not sure.

I will be kind and polite to everyone online.

I will tell a trusted adult if I feel worried, scared or nervous when I am using a device.
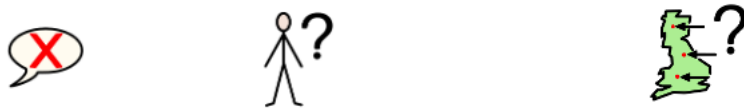
I will tell a trusted adult if I feel sad, angry or embarrassed when I am using a device.

I will tell a trusted adult if I feel bad or unsafe when I am using a device.

I know people online sometimes tell lies.

They might lie about who they are or where they live.

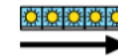I never have to keep secrets from my trusted adults.

I will not change clothes or undress in front of a webcam.

I will always ask a trusted adult before telling anyone my private information or location.

I know that anything I do or say online might stay there forever.

It can be given to my family, my friends or strangers.

This could make me feel sad or embarrassed.

My trusted adults are _____ at school

My trusted adults are _____ at home

My name is _____

Appendix 6: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	