MARNER
PRIMARY SCHOOL

Online Safety Policy

Introduction

School Name: Marner Primary
Date policy was approved: May 2025
Review date: May 2027
Person responsible for overseeing Online Safety: **Carol Doherty**
Person writing this policy: **Carol Doherty**

Key People/dates

	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Carol Doherty
	Deputy Designated Safeguarding Leads / DSL Team Members	Sarah Bowmer, Jane Scott Gall
	Link governor for safeguarding and web filtering	Helen Witty
	Curriculum leads with relevance to online safeguarding and their role	Yasmina Bibi – PSHE Lead Stuart Seamark – Wellbeing Lead
	Network manager / other technical support	School Business Services
	Date this policy was reviewed and by whom	November 2025 – Sam Sharpe
	Date of next review and by whom	October 2026

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' 2024 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils

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

Who is in charge of online safety?

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

What are the main online safety risks in 2025?

Current Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

TikTok – Children having access to and using TikTok. You must be 13 years old to use TikTok and the content is managed for older children.

Discord - Children using this app to group chat online. This has brought up online bullying issues.

Misogynistic Influencers using youtube to promote inappropriate language and relationships.

Nationally, some of the latest trends of the past twelve months are outlined below. These are reflected in this policy and the acceptable use agreements we use and seen in the context of the 5 Cs (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

Last year, we highlighted the rapid rise of generative AI (GenAI). Since then, the trend has exploded. Thousands of sites now offer AI-generated content, including disturbing levels of abusive, pornographic, and even illegal material like child sexual abuse content. Some platforms host AI "girlfriends," unregulated therapy bots, and even chatbots that encourage self-harm or suicide—tools many students can access freely at home or school. Chatbots can also blur reality, offering harmful advice or engaging in sexualised and bullying conversations. Their addictive design and unmoderated nature heighten the risk of overuse and exploitation.

When used for generating text, GenAI presents multiple risks. It can spread misinformation, facilitate plagiarism, and most worryingly, bypass safety settings. Many tools lack effective age controls and produce inappropriate content.

Beyond text, GenAI makes it easier than ever to create sexualised images and deepfake videos. These can have a devastating emotional and physical impact on young people, including blackmail and abuse. The Internet Watch Foundation has warned of a sharp rise in AI-generated child sexual abuse imagery. Alarming reports also show children using nudifying apps to create illegal content of peers.

We regularly see AI searches involving sexualised and harmful content. It's critical to stress that in the UK, any CSAM (child sexual abuse material)—AI-generated, photographic, or even cartoon—is illegal to create, possess, or share.

Schools must address this not just in the classroom, but by educating parents and students on safe use at home.

Ofcom's 'Children and parents: media use and attitudes report 2025' has shown that YouTube remains the most used site or app among all under 18s, followed by WhatsApp, TikTok, Snapchat and Instagram. With children aged 8-14 spending an average of 2 hours 59 minutes a day online across smartphone, tablet and computer – with girls spending more time online than boys, four in ten parents continue to report finding it hard to control their child's screentime. Notably, 52% of 8-11s feel that their parents' screentime is also too high, underlining the importance of modelling good behaviour.

Given the 13yrs+ minimum age requirement on most social media platforms, it is notable that over half of 3-12-year olds (55%) were reported using at least one app. Despite age restrictions, four in ten admit to giving a fake age online, exposing them to content inappropriate for their age and increasing their risk of harm, with over a third of parents of all 3-17s saying they would allow their child to have a profile on sites or apps before they had reached the minimum age.

We have also come across online communications platforms that offer anonymous chat services and connect users with random strangers allowing text and video chats. Most of these are easily accessible to children on devices.

As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore will remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that 25% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3- to 6-year-olds are being tricked into 'self-generated' sexual

content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and for the first time there were more 7–10-year-olds visible in child sexual abuse material (CSAM) images than 11-13s.

Growing numbers of children and young people are using social media and apps such as Snapchat as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news. The alarming speed and scale at which misinformation about the attack in Southport (August 2024) was shared, resulting in Islamophobic and racist violence, rioting and looting across England is particularly concerning, with much of it fuelled by false online accusations about the assailant. Despite attempts by Police and national news to correct the misleading information, it racked up millions of views on social media sites like X and was actively promoted by several high-profile users with large followings.

Growing numbers of children and young people are using social media and apps, primarily TikTok as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news.

There have also been significant safeguarding concerns where parents have filmed interactions with staff outside the school gates and posted this on social media, putting children and the wider school community at risk of harm.

Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2025 highlighting an increase in school attacks nationally, with 60% of secondary schools reporting a breach or attack in the past year, and 44% of primary schools.

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 <u>all</u> 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

Overview

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

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

Further help and support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with Marner Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding Teams (MAST) and normally the headteacher will handle referrals to the LA designated officer (LADO).

Scope

This policy applies to all members of the Marner Primary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils,

parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

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

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

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

Education and curriculum

Despite the risks associated with being online, Marner Primary School recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

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.

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

The teaching of online safety, features in these particular areas of curriculum delivery:

- Relationships education, relationships and sex education (RSE)
- 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 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, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

At Marner Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

teachcomputing.org

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access.

Handling safeguarding concerns and incidents
It is vital that all staff recognise that online safety is a part of safeguarding and so 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 speak to the safeguarding lead with any concerns (no matter how small these seem) 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):

- *Safeguarding and Child Protection Policy*
- *Anti-Bullying Policy*
- *Behaviour Policy (including school sanctions)*
- *Acceptable Use Policies*
- *Prevent Risk Assessment / Policy*
- *Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)*
- *Cyber Security*

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

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMS - this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

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

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

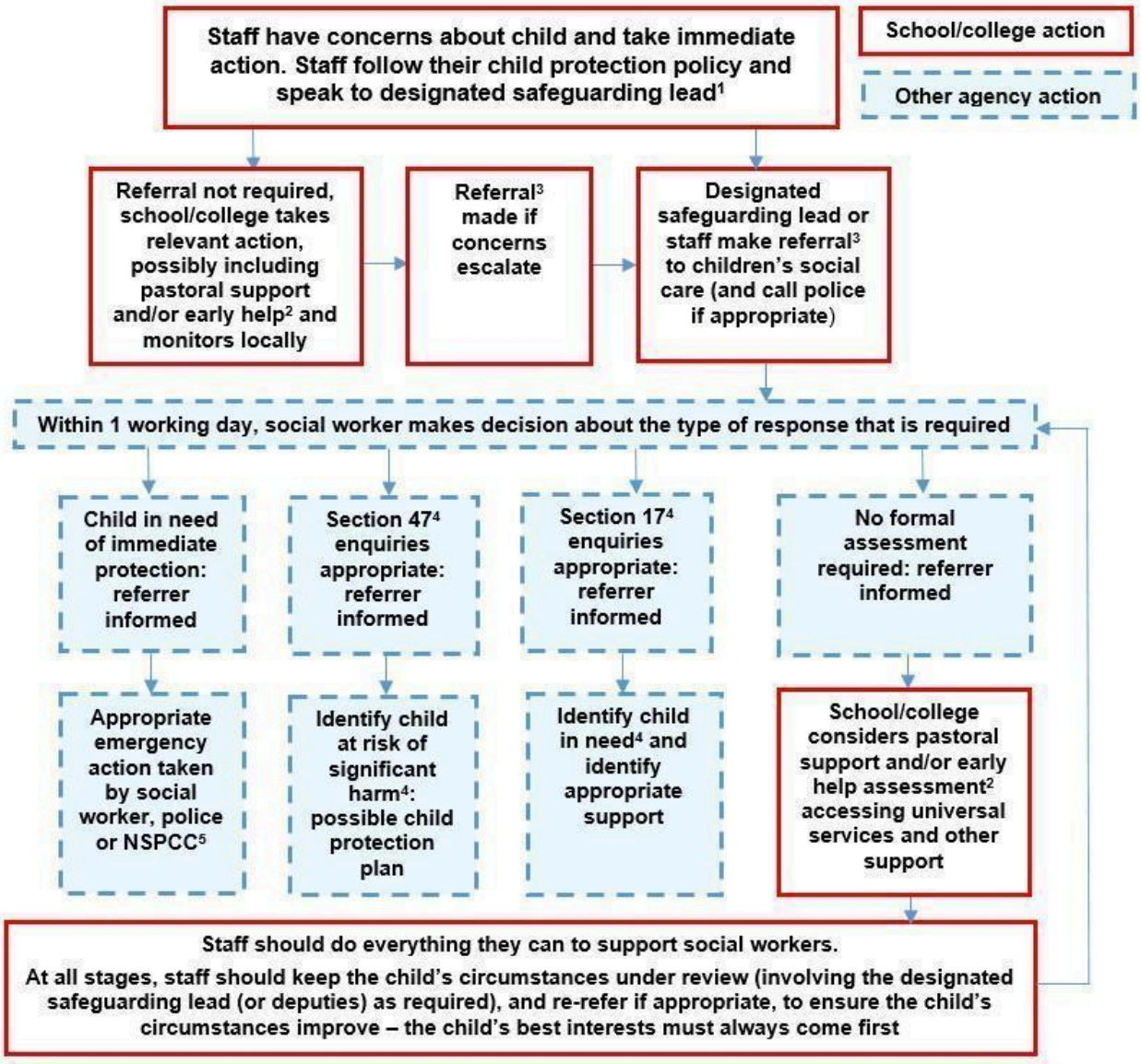
We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

For more information on reporting channels for online safety concerns, please visit reporting.lgfl.net.

Actions where there are concerns about a child

The following flow chart 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.



Nudes -sharing nudes and semi-nudes

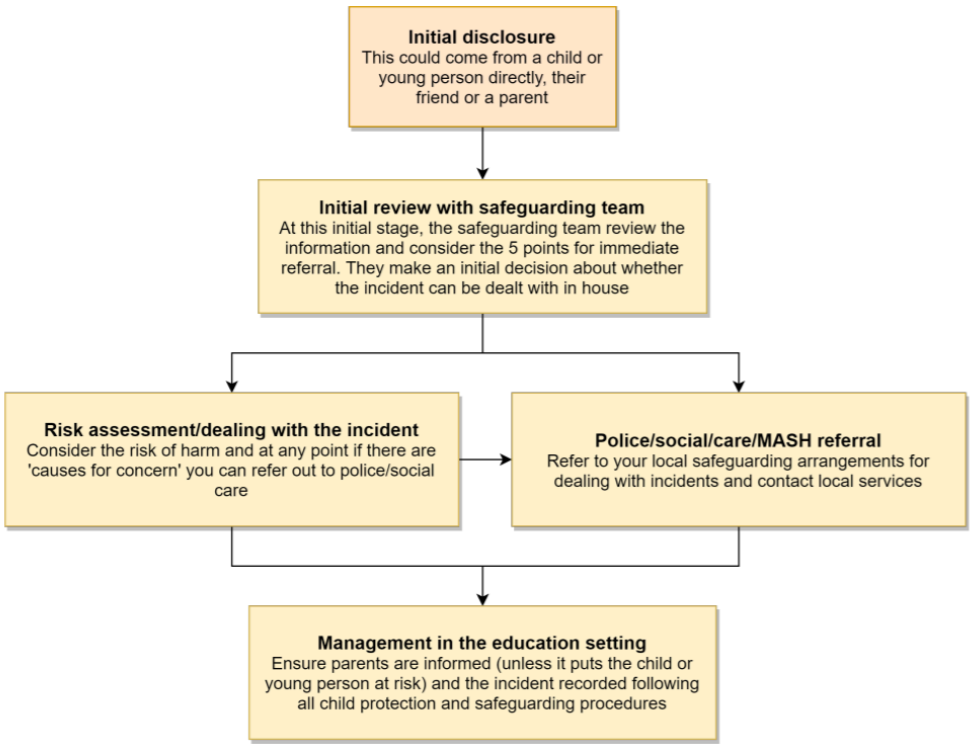
All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings

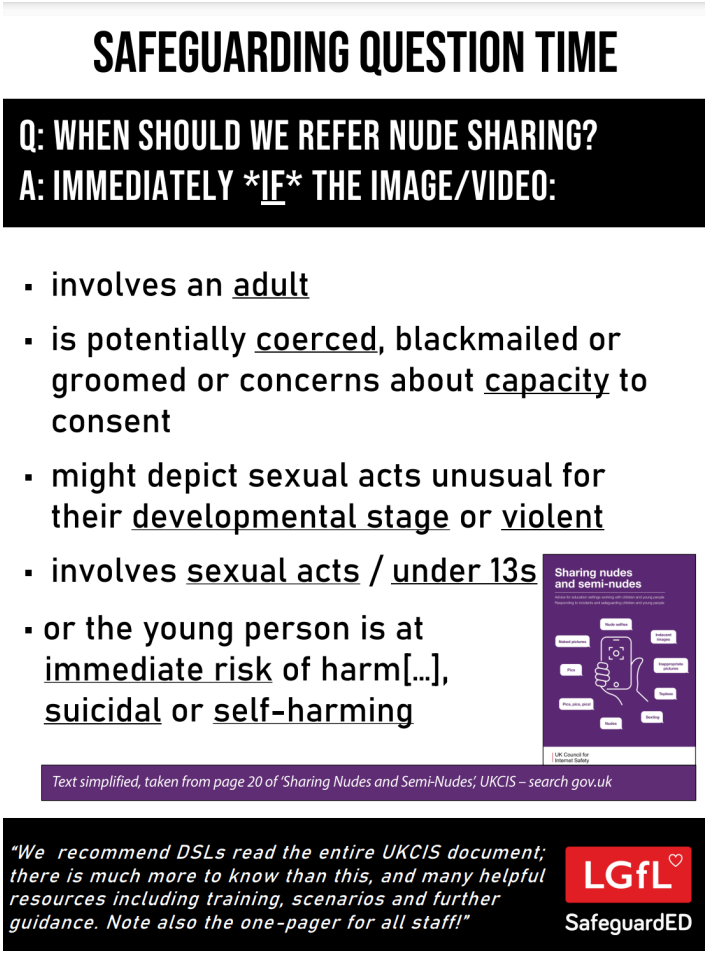
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of 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.**

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

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.

The following LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:





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 (which may also be referred to as cyberbullying), 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. This includes issues arising from banter.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

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

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. 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 the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

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

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

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

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy/online safety.

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

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Marner Primary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cybersecurity policy. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for schools and colleges.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2025, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with School Business Services to implement the DfE filtering and monitoring standards, which require schools to:

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

We provide appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times through SENSO.

We ensure all staff are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via CPOMS and will be asked for feedback at the time of the regular checks which will now take place.

Technical and safeguarding colleagues work together closely to carry out annual reviews and checks and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc.

At our school we recognise that generative AI sites can pose data risks so staff are not allowed to enter child data and where they use them, they must be approved. For children and young people, we block the generative AI category and only allow specific sites. We know that what children input and what the tool outputs cannot be guaranteed as safe and inappropriate content can be generated, so we carefully monitor output and limit their use - also in line with DfE guidelines.

SafeSearch is enforced on any accessible search engines on all devices.

Please note that our monitoring and filtering alert service only works on devices at Marner Primary. We can monitor content that travels through the school based google logins (given to all children at Marner) on home devices but alerts are not monitored during weekends and holidays.

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

At Marner Primary School:

- *web filtering is provided by Webscreen through LGFL on the school site*
- *Monitoring is provided by Senso and is monitored by the DSL team.*
- *Overall responsibility is held by the DSL with further support from Sam Sharpe.*
- *technical support and advice, setup and configuration are from Edward Hall through SBS.*
- *Regular checks are made half termly by Edward Hall to ensure filtering is still active and functioning everywhere. These are evidenced in visit reports emailed to Sam Sharpe, Sarah Bowmer (headteacher) and the administration team at Marner Primary School.*
- *an annual review is carried out*

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

- p*hysically monitoring by staff watching screens of users*
- *live supervision by staff on a console with device management software*
- *network monitoring using log files of internet traffic and web access*

- *individual device monitoring through software or third-party services*

At Marner Primary School we use *Google for Education*

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

Authorised systems
Pupils at this school communicate with each other and with staff using Google Classroom.

Staff at this school use the email system provided by Google for Education and our School Management Information system (MIS), Arbor for all school emails. They also use ClassDojo to communicate with parents and families. They never use a personal/private email account to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.

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

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

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

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour/usage principles of messaging/commenting systems

Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying,

aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy only using the authorised systems mentioned above.

Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Use of generative AI

At Marner we acknowledge that generative AI platforms (e.g. ChatGPT or Gemini for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- *We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons.*
- *We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deep fakes, undressing apps).*
- *The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.*
- *We are currently trialling different AI software (Education based) to support with marking and planning. Staff request use of a new platform for approval to Sam Sharpe. Parent workshops will take place throughout the year to educate our community on the dangerous use of AI*

Online storage or learning platforms

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

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Any new platforms will be approved by Sam Sharpe.

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 site is managed by Juniper Websites

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

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.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Marner Primary School members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on Google Drive in line with the retention schedule of the school Data Protection Policy. Any concerns about the nature of these images will be reported to the DSL

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 (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

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

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

Social media

Our SM presence

Marner 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.

Negative coverage almost always causes some level of disruption.

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.

The Senior Leadership Team are responsible for the school's social media accounts and checking our Wikipedia and Google reviews and other mentions online.

Staff, pupils' and parents' SM presence

Social media (including 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 but the school regularly deals with issues arising on social media involving 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). We refer to the 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 the Children's Commission Digital 5 A Day.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

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) as laid out in the AUPs. 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 there has been a significant number of 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 and permission is sought before uploading photographs, videos or any other information about other people. Parents must not covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Device usage

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

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

- *Pupils/students are allowed to bring mobile phones in for emergency use only. These must be handed to the school office on entry to the school and will be returned on leaving.*
- *All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies. 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 should inform the phase leader.*
- *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. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.*
- *Neither staff nor students are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.*

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wifi is accessible to visitors for school related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

All and any usage of devices and/or systems and platforms may be tracked.

Trips/events away from school

For school trips/events away from school, teachers will use their own mobile phones to contact school/ The school will then contact parents. Any deviation from this policy (e.g. by mistake or because the phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Appendix - Roles

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

All school staff must read the "All Staff" section as well as any other relevant to specialist roles

Roles:

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

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2024) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL about overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Headteacher - Sarah Bowmer

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*
- *Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles*
- *Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.*
- *Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information*
- *Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards*
- *Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information*
- *Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident*
- *Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised*
- *Ensure the school website meets statutory requirements*

Designated Safeguarding Lead/Online Safety Lead - Carol Doherty

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

- *The DSL should "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).*

- *Ensure "An effective whole school approach to online safety as per KCSIE*
- *Ensure the school is complying with the DfE's standards on Filtering and Monitoring.*
- *As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc*
- *Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused*
- *Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.*
    - *This must include filtering and monitoring and help them to understand their roles.*
    - *All staff must read KCSIE Part 1 and all those working with children also Annex B*
    - *Cascade knowledge of risks and opportunities throughout the organisation.*
- *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*
- *Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns*
- *Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language (see spotlight.lgfl.net for a resource to use with staff on how framing things linguistically can have a safeguarding impact, and some expressions we use might be unhelpful)*
- *Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behaviour apply*
- *Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)*
- *Work with the headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information*
- *Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.*
- *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*

- *Ensure that online-safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life*
- Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents, including hard-to-reach parents
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to online tutors, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents.

Governing Body, led by Online Safety/Safeguarding Link Governor - Helen Witty

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*
- *Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated*
- *Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards*
- *Support the school in encouraging parents and the wider community to become engaged in online safety activities*
- *Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings*
- *Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information*

- *Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B*
- *Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring*
- *"Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."*

PSHE/RSHE Lead(s) - Yasmina Bibi - PSHE, Stuart Seamark - Wellbeing

Key responsibilities:

- *As listed in the 'all staff' section, plus*:
- *Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."*
- *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"*
- *Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.*
- *Note that an RSHE policy should be included on the school website.*
- *Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach*

Computing - Sam Sharpe

Key responsibilities:

- *As listed in the 'all staff' section, plus*:
- *Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum*
- *Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach*

- *Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing*
- *Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements*

Subject/aspect leaders

Key responsibilities:

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

Network Manager/other technical support roles - Edward Hall - SBS

Key responsibilities:

- *As listed in the 'all staff' section, plus*:
- *Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.*
- *Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks*
- *Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards protections for pupils in the home and remote-learning.*
- *Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.*
- *Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.*
- *Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive*

records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.

- *Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.*
- *Maintain up-to-date documentation of the school's online security and technical procedures.*
- *To report online safety related issues that come to their attention in line with school policy.*
- *Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.*
- *Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable*
- *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.*
- *Work with the Headteacher to ensure the school website meets statutory DfE requirements*

Data Protection Officer (DPO) - Louise Manthorpe, Specialist Redaction Services

Key responsibilities:

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

Volunteers and contractors (including tutor)

Key responsibilities:

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

Pupils

Key responsibilities:

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

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it

External groups including parent associations

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*

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

Background

We ask everyone involved in the life of Marner Primary School 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 staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. 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 If you have any questions about this AUP or our approach to online safety, please speak Sam Sharpe (Strategic IT Lead) or Carol Doherty (DSL)

What am I agreeing to?

I have read and understood Marner Primary School'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 as outlined in the Online Safety Policy.

1. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
2. I 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) and make them aware of new trends and patterns that I identify.
3. I will follow the guidance in the Safeguarding and Online Safety policies for reporting Incidents (including for handling 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 understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom. understand the sections on.
5. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it couldhappen here'!

6. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, 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).
7. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
8. I will check with Sam Sharpe if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured.
9. I will follow best-practice pedagogy for online safety education, avoiding scarring and other unhelpful prevention methods.
10. I will prepare and check all online sources and classroom resources before using them, for accuracy and appropriateness. I will flag any concerns about "overblocking" to the DSL.
11. I will 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 data protection.
12. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
13. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
14. 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.
15. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.
16. 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 both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
17. 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.

18. If I already have a personal relationship with a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.

19. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am ever not sure, I will ask first.

20. I will not use any new technology or download any apps without agreement from Sam Sharpe

21. I will not use a mobile hotspot to provide internet to any device I use in school.

22. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.

23. 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.

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

25. I will only use gen AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation

STAFF, GOVERNORS, VOLUNTEERS

Background

We ask everyone involved in the life of Marner Primary School to sign an Acceptable Use* Agreement (AUA), 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 AUA is reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. 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

If you have any questions about this AUA or our approach to online safety, please speak Sam Sharpe (Strategic IT Lead) or Carol Doherty (DSL)

What am I agreeing to?

I have read and understood Marner Primary School'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 as outlined in the Online Safety Policy.

1. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
2. I 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) and make them aware of new trends and patterns that I identify.
3. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling 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 understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom. understand the sections on.
5. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'!

6. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, 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).
7. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
8. I will check with Sam Sharpe if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured.
9. I will follow best-practice pedagogy for online safety education, avoiding scarring and other unhelpful prevention methods.
10. I will prepare and check all online sources and classroom resources before using them, for accuracy and appropriateness. I will flag any concerns about "overblocking" to the DSL.
11. I will 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 data protection.
12. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
13. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
14. 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.
15. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.
16. 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 both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
17. 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.

18. If I already have a personal relationship with a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.
19. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am ever not sure, I will ask first.
20. I will not use any new technology or download any apps without agreement from Sam Sharpe
21. I will not use a mobile hotspot to provide internet to any device I use in school.
22. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.
23. 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.
24. 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. I understand that any breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
25. I will only use gen AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.

MARNER
PRIMARY SCHOOL

Acceptable Use Agreement (AUA) for
EYFS and KS1 PUPILS

My Class is called:

_____

To stay SAFE online and on my devices, I follow the Digital 5 A Day and:	✔
1. *I only USE devices or apps, sites or games if I am allowed to*	
2. *I ASK for help if I'm stuck or not sure; I TELL a trusted adult if I'm upset, worried, scared or confused*	
3. *I look out for my FRIENDS and tell someone if they need help*	
4. *If I get a FUNNY FEELING in my tummy, I talk to an adult*	
5. *I KNOW that online people aren't always who they say they are and things I read are not always TRUE*	
6. *Anything I do online can be shared and might stay online FOREVER*	
7. *I don't keep SECRETS 🚫 unless they are a present or nice surprise*	
8. *I don't have to do DARES OR CHALLENGES ❌, even if someone tells me I must.*	
9. *I don't change CLOTHES or get undressed in front of a camera*	
10. *I always check before SHARING my personal information or other people's stories and photos*	
11. *I am KIND and polite to everyone*	

Our trusted adults are:

_____ *at Marner Primary School*

We have talked about our trusted adults at home. We can tell you about them if you ask us individually.

www.childrenscommissioner.gov.uk/digital/5-a-day/

Appendix iv

LGfL SafeguardED

MARNER PRIMARY SCHOOL

Acceptable Use Agreement (AUA) for
KS2 PUPILS

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

- *I learn online – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.*
- *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.*
- *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. If I'm not sure, I will ask.*
- *I am creative online – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.*
- *I am a good friend online – I won't share or say anything I know would upset another person or they wouldn't want to share. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.*
- *I am not a bully – I know just calling something fun or banter doesn't stop it hurting someone else. 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.*
- *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!*
- *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.*
- *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.*
- *If I make a mistake I don't try to hide it but ask for help.*
- *I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.*
- *I know 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.*
- *I never pretend to be someone else online – it can be upsetting or even dangerous.*
- *I check with a parent/carer before I meet an online friend the first time; I never go alone.*
- *I don't go live (videos anyone can see) 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.*

- *I don't take photos or videos or people without them knowing or agreeing to it – and I don't create artificial images, videos or deep fakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.*
- *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.*
- *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.*
- *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.*
- *I follow age rules – 13+ games, apps and films 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.*
- *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.*
- *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).*
- *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.*
- *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.*
- *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.*
- *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, and I know which sites to trust, and how to double check information I come across. 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.

I can choose the people who I most trust to help me.

At school that might mean _____

Outside school, my trusted adults are_____

I know I can also get in touch with Childline

Signed: _____ Date: _____