Congerstone Primary School

Online Safety Policy

Status	Active
Sources	London Grid For Learning Policy 2023
Version	Oct 23
Governors committee	All Governors
Consultation Period	Nov 23
Date approved	8.12.23
Date of next review	Aug 2023
Target group	Everyone- staff, governors, parents
Linked policies	Child Protection and Safeguarding Policy Anti Bullying Policy Data Protection Policy
Signed – Chair of Governors	
Signed – Headteacher	

Document History:

Version	**Date of Review**	**Reviewed by:**	**Revisions made:**
Oct 23	Aug 24	JA/GK/AR	New policy inline with KCSIE 2023

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Alison Ruff
	Deputy Designated Safeguarding Leads / DSL Team Members	Claire Simpson
	Link governor for safeguarding	Hannah Wood
	Curriculum leads with relevance to online safeguarding and their role	PSHE – Alison Ruff Computing – Jodie Armstrong
	Network manager / other technical support	Gavin King
	Date this policy was reviewed and by whom	Alison Ruff Jodie Armstrong
	Date of next review and by whom	Alison Ruff Jodie Armstrong Autumn term 2024

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into our 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 school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all 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. 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 PSHE, will plan the curriculum for their area, it is important that this ties into a whole-school approach.

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

Current Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students: This includes but not limited to sending unkind messages on, for example, Whatsapp, and sharing photographs of each other without permission.

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

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

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

The continued cost-of-living crisis has meant children have spent more time online and therefore exposed to all manner of online harms as families have had to cut back on leisure activities and public provision of free activities for young people has reduced further.

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

This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

How will this policy be communicated?

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

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

Contents

Overview

Aims

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

- Setting out expectations for all Congerstone 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 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 school, supporting our 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 for reporting and support should always be followed first, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding team and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority or third-party support organisations you work with may also have advisors to offer general support.

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

Scope

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

Roles and responsibilities

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

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

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

Education and curriculum

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

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils – dedicated training around this with curriculum mapping for RSHE/PSHE and online safety leads is available at safetraining.lgfl.net

RSHE guidance also recommends schools assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress." [See LGfL's SafeSkills Online Safety Quiz and diagnostic teaching tool which is linked to statements from UKCIS Education for a Connected World framework, enabling teachers to monitor progress throughout the year and drill down to school, class and pupil level to identify areas for development at **safeskillsinfo.lgfl.net**]

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

- Relationships education, relationships and sex education (RSE) and health (also known as PSHE)
- Computing
- Citizenship (aspects within LMTW and PSHE)

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

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

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

At Congerstone 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.

This is done within the context of an annual online safety audit, which is a collaborative effort led by Jodie Armstrong (Computing Lead) and Hannah Wood (Safeguarding and Anti-bullying governor).

Handling safeguarding concerns and incidents

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

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

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

School procedures for dealing with online safety are mostly detailed in the following policies

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

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 school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through school's escalation processes.

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

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline (you may want to display a poster with details of this / other helplines in the staff room – see posters.lgfl.net and reporting.lgfl.net).

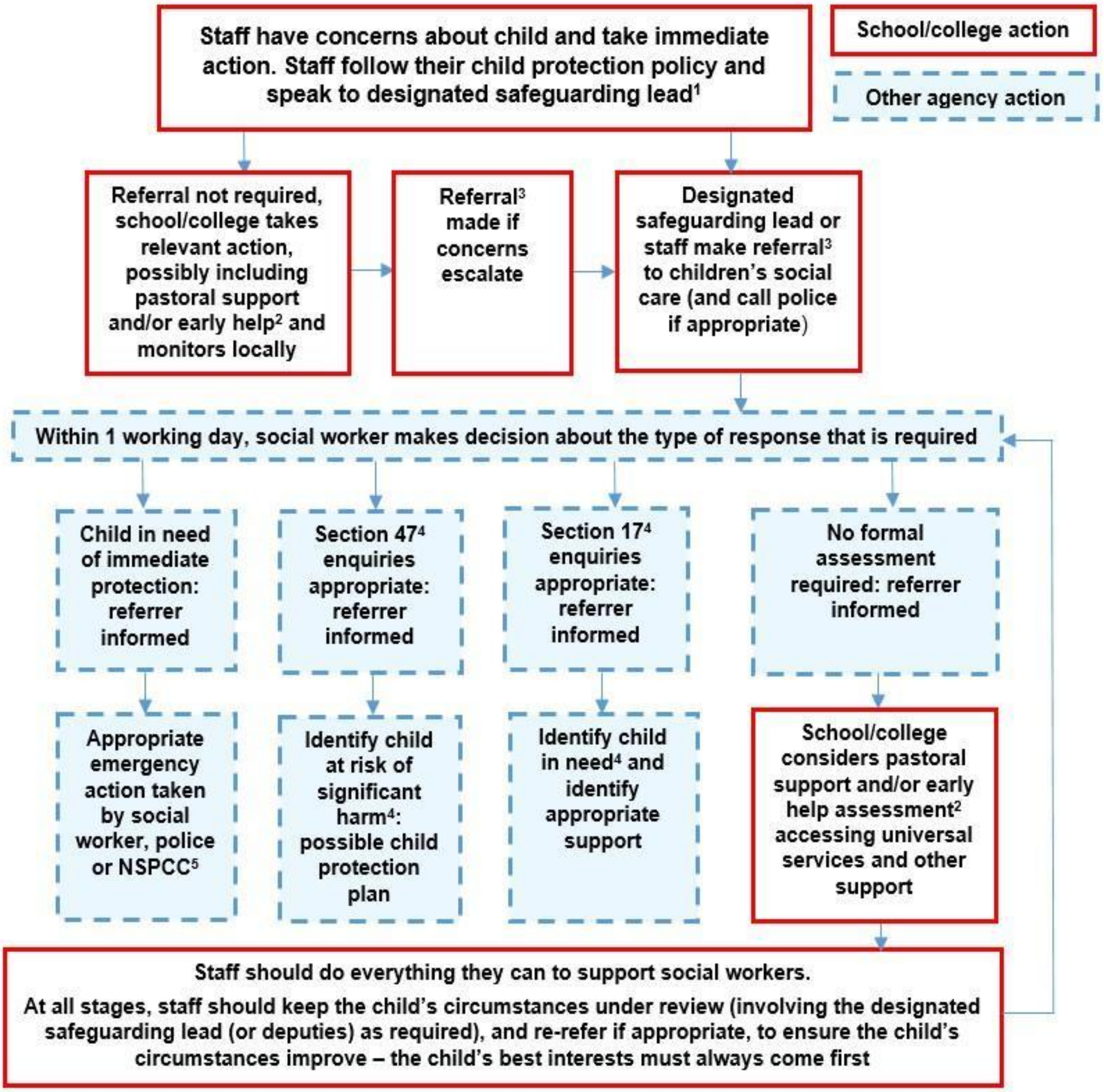
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents.

We may 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).

School will evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart is from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. Remember online safety concerns are no different to any other safeguarding concern.



School/college action

Other agency action

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]

Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally

Referral[3] made if concerns escalate

Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)

Within 1 working day, social worker makes decision about the type of response that is required

Child in need of immediate protection: referrer informed

Section 47[4] enquiries appropriate: referrer informed

Section 17[4] enquiries appropriate: referrer informed

No formal assessment required: referrer informed

Appropriate emergency action taken by social worker, police or NSPCC[5]

Identify child at risk of significant harm[4]: possible child protection plan

Identify child in need[4] and identify appropriate support

School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support

Staff should do everything they can to support social workers.

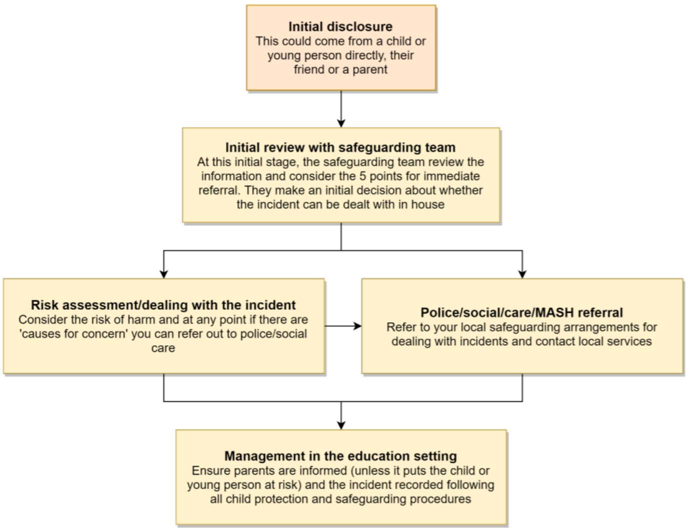
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Sexting – sharing nudes and semi-nudes

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

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

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



Initial disclosure
This could come from a child or young person directly, their friend or a parent

Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house

Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care

Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services

Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

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

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

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

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

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

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

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

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' and it would be useful for all staff to be aware of many aspects outlined there to support a whole-school response; case studies are also helpful for training.

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

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

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 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.

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 **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

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

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Congerstone Primary school community. These are also governed by school Acceptable Use Policies the school's social media policy and within the staff handbook.

Breaches will be dealt with in line with the behaviour policy (for pupils) or code of conduct 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, Congerstone Primary School will reques the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, 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.

Data protection

All pupils, staff, governors, volunteers, contractors and parents are bound by the data protection policy. It is important to remember there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

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." KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

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

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

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

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

As schools get to grips with new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via CPOMS and will be asked for feedback at the time regular checks take place.

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

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

At Congerstone Primary School

- web filtering is provided by RM using RM SafetyNet for all devices connected to the school network while on site.
- changes can be made by Gavin King and Alison Ruff
- overall responsibility is held by the DSL, Alison Ruff
- technical support and advice, setup and configuration are from Gavin King, GSKS
- regular checks are made half termly by Gavin King, GSKS to ensure filtering is still active and functioning everywhere.
- an annual review is carried out as part of the online safety audit to ensure a whole school approach.

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

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

At Congerstone Primary School, we use staff supervision as our primary monitoring strategy, which is supplemented by the use of Senso Cloud Safeguarding to capture screen grabs of potentially inappropriate material on devices.

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

Authorised systems

- Pupils at this school communicate with staff using Seesaw. This platform is used to upload homework, where teachers are able to comment and give praise/support as necessary. Concerns and appointments from parents should be requested via the school office through the landline or, ideally, email. User guidance regarding Seesaw is sent out annually.
- Staff at this school use the email system provided by Microsoft 365 for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when related to school/child data, using a non-school-administered system.

Any systems above are centrally managed and administered by school or authorised IT partner Gavin King, GSKS (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for 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.

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff code of conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring 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 Data Protection Policy and only using authorised systems mentioned above.
- Pupils were allocated an email as a means to login to Teams during lockdown.

Online storage or learning platforms

All 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. Congerstone Primary School has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times.

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 Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to Caroline Hunter

Our site is hosted by Wix.

Where staff submit information for the website, they are asked to remember schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. 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 Caroline Hunter or Gavin King.

Digital images and video

When a pupil joins our school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer with regard to:

- Promotional publicity
- Social Media
- School prospectus

- Local publications (such as *The Graphic)*
- Display boards and use within school
- School website
- Photography for home purchase

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

Photos are stored on the local network, in SharePoint or on encrypted staff iPads in line with the retention schedule of the Data Protection Policy, except for images and videos uploaded to social media which will slide down the continuous feed.

Staff and parents are reminded annually and before school performances 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 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

Congerstone 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 school online). Few parents will apply for a school place without first Googling school, and the Ofsted pre-inspection check includes monitoring what is being said online.

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

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 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 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 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 our 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 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 school reputation (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but school has dealt with issues arising on social media involving Primary aged pupils (under the age of 13). We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, 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 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. Children 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). The following documents may support you to establish shared expectations within your family: Digital Family Agreement; Top Tips for Parents; parentsafe.lgfl.net; and, Children's Commission Digital 5 A Day.

The school has official Facebook, X-Twitter and Instagram accounts, which are used as one-way communication to share information about what pupils have been learning, key message and the sharing of successes. Congerstone Primary School will not respond to messages about children through social media and parents/carers should communicate these messages via the school office.

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

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils 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, staff must not follow such public pupil 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 they are obliged not to bring 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 school or its stakeholders on social media and be careful that their personal opinions are not be attributed to school, or local authority, thus bringing 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 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.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

AUPs remind those with access to school devices about rules on misuse of school technology – devices used at home should be used just like 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** are not allowed to bring in their own devices into school. Important messages and phone calls to or from parents can be made via the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and, in most cases, only use their devices in staff-only areas. Staff are required to use their phones for two-factor authentication when accessing their Email. Staff may also be expecting an important phone call, in which case, the Headteacher should be informed.
- **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 follow our Photography policy when attending school events such as school performances, assemblies and sports days. Posters in the hall provide a visual reminder and the policy is readily available at performances and sports days.

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 authorised staff and guests 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 pupils are restricted to the apps/software installed by school, whether for use at home or school, and may be used for learning, as well as reasonable, 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 be issued a school duty phone and this number should be used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes 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.

Full details of the school's search procedures are available in the school Behaviour Policy.

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, contractors, music teachers and coaches
- 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/staff handbook 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 start of document for issues in 2023) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

Headteacher – Alison Ruff

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support activities of the designated safeguarding lead team and ensure they work with 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 school's arrangements
- Ensure 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 new DfE standards—through regular liaison with technical colleagues and DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.

    - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring 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 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 – Alison Ruff (DSL) and Claire Simpson (Deputy DSL)

Key responsibilities (DSL can delegate certain online-safety duties but not 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
- In 2023/4 work to take up the new responsibility for filtering and monitoring by working closely with technical colleagues, SLT and the new filtering governor to learn more about this area, better understand, review and drive the rationale behind systems in place and initiate regular checks and annual reviews, including support for devices in the home.
- 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. PSHE, Computing), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - In 2023/4 this must include filtering and monitoring and help them understand their roles
    - all staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net (B the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)
    - cascade knowledge of risks and opportunities throughout the organisation
    - safecpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- Ensure ALL governors 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
- 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 headteacher, DPO and governors to ensure a compliant framework for storing data, but helping to ensure child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with latest trends in online safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates in online-safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure 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 school community, with a strong focus on parents, including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of 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).

Governing Body, led by Online Safety / Safeguarding Link Governor – Jodie Armstrong (staff governor and Computing Lead, and Hannah Wood, Parent governor, Safeguarding governor and Anti-bullying governor.

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 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 all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Ensure filtering and monitoring is part of the role for Jodie Armstrong and Hannah Wood and they work closely with the DSL and Technical Support Advisor on the new filtering and monitoring standards
- Support school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with 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 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 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 approach to online safety [with] a clear policy on the use of mobile technology."

PSHE / Lead – Alison Ruff

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 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.
- Work closely with DSL/OSL and all other staff to ensure an understanding of issues, approaches and messaging within PSHE / RSHE.
- Note that an PSHE/RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – Jodie Armstrong

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the PSHE 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 as appropriate.

Network Manager/other technical support roles – Gavin King, GSKS

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE.
- 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 / PSHE lead to ensure school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy

- Manage 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 data protection policy and cybersecurity policy are up to date, easy to follow and practicable
- Monitor 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) – Warwickshire DPO (up to Jan 24) GDPR Service for Schools (GDPRSS- Leics) (after Jan 2024)

Due to the transition period of provider this will be reviewed as required at a later date

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 policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records.
- Ensure all access to safeguarding data is limited as appropriate, and also monitored and audited

Staff who work in school but are not employees e.g music teachers and coaches

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

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

- Understand Congerstone Primary School use social media as one-way communication to share successes
- Follow the learning platform guidelines outlined at the beginning of the year (example, do not upload faces of pupils to Seesaw when photographing homework)
- Follow photography restrictions and guidelines.

External groups including parent associations (Friends of Congerstone)

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