



Cranbrook Primary School

Online Safety Policy

Approved by the Governing Body on:

Review Date: Autumn 2026

Chair of Governors signature: Debbie Wiles

Introduction

Key people / dates

Cranbrook Primary School 	Designated Safeguarding Lead (DSL) team	Kimberly McKoy
	Online-safety / safeguarding link governor	Debbie Wiles
	RSHE lead	Khaium Miah / Samantha Patel
	Date this policy was reviewed	Autumn 2025
	Date of next review and by whom	Autumn 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. This policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE 2025), 'Teaching Online Safety in Schools' statutory RSHE guidance and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing. It is designed to sit alongside our school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

What were the main online safety risks in 2024/2025?

Current Online Safeguarding Trends

At our school, we classify Online Safety incidents based on the following categories: Cyber Incident/ Cyber bullying and Online Safety. The cyber incidents are gaming related or social media platforms.

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. For guidance and resources, visit genai.lgfl.net.

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.

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 the 7–10-year-old age group remains the fastest growing for this form of child sexual abuse material.

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 was 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.

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. See nofilming.lgfl.net to find out more.

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

2024 highlighting an increase in school attacks nationally, with 71% of secondary schools reporting a breach or attack in the past year, and 52% of primary schools.

The continued cost-of-living crisis has meant that 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 the public provision of free activities for young people has reduced further.

How will this policy be communicated?

This policy can only impact upon practice if it is a 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
 - Available on the internal staff network/drive
 - Available in paper format in the staffroom
 - 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).
 - AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
 - AUPs are displayed in appropriate classrooms (not just in Computing corridors/classrooms)
- APPENDIX 1 and 2.

Contents

Contents

Online Safety Policy1

Contents.....5

Overview.....7

Aims.....7

Further Help and Support8

Scope.....8

Roles and responsibilities8

Education and curriculum	9
Handling online-safety concerns and incidents	10
Nudes – sharing nudes and semi-nudes	12
Upskirting	13
Bullying	13
Child-on-child sexual violence and harassment	14
Misuse of school technology (devices, systems, networks or platforms)	14
Social media incidents	15
CCTV	15
Extremism	15
Data protection and cyber security	16
Appropriate filtering and monitoring	16
Messaging/commenting systems (incl. email, learning platforms and more)	17
Use of generative AI	18
Online storage and learning platforms	19
School website	19
Online storage or learning platforms	19
Digital images and video	20
Staff, pupils' and parents' SM presence	22
Device usage	23
Personal devices including wearable technology and bring your own device (BYOD)	23
Use of school devices	24
Network / internet access on school devices	25
Trips / events away from school	25
Searching and confiscation	25
Searching children suspected of having prohibited items	25
Appendix A- Acceptable Use Policies	25
Appendix B – Roles	26
All staff	26
Headteacher – Cassim Bana	28
Designated Safeguarding Lead / Online Safety Lead –Kimberly McKoy	29
Governing Body, led by Online Safety / Safeguarding Link Governor – Debbie Wiles	30
PSHE/RSHE Lead – [Khaium Miah/Samantha Patel]	31

Computing Lead – Khaium Miah.....	31
Subject Leaders	32
Network Manager/Technician	33
Data Protection Officer (DPO) – David Powell.....	34
Volunteers and contractors (including online tutors)	35
Pupils.....	35
External groups including parent associations – CFA	35

Overview

Aims

This policy aims to:

- Set out expectations for all Cranbrook Primary School community members’ online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues
- Help 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, and regardless of device or platform and that the same standards of behaviour apply online and offline.

- Facilitate 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
- Help 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
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Further Help and Support

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

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 new 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 the Cranbrook Primary School community (including teaching and support staff, supply staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether onsite 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 Appendix B 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 2025/2026, 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, Cranbrook 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 develops competencies (as well as knowledge about risks) and 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 that schools assess teaching to identify where pupils need extra support or intervention.

The following subjects have the clearest online safety links:

- Relationships, Sex and Health Education (RSHE) and 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 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 tasks

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. 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 Cranbrook 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.

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 online-safety concerns and incidents

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

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 onlinesafety 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 all forms of bullying, 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 (GDPR) Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc.)
- Cybersecurity

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

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

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

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

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

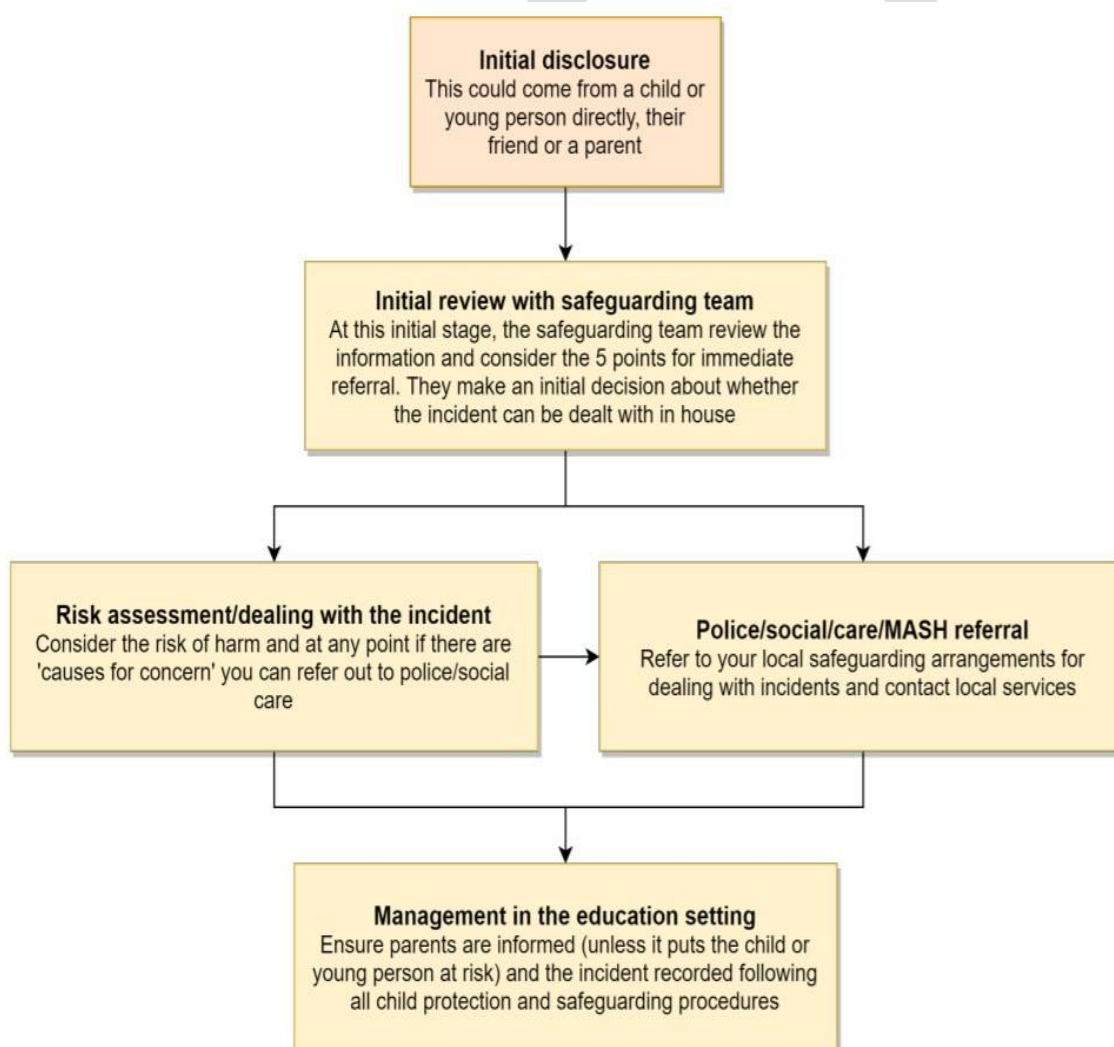
The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc. and make alternative provisions in advance where these might be needed.

Nudes – sharing nudes and semi-nudes

At Cranbrook Primary we refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings

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

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



SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?

A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

- involves an adult
- is potentially coerced, blackmailed or groomed or concerns about capacity to consent
- might depict sexual acts unusual for their developmental stage or violent
- involves sexual acts / under 13s
- or the young person is at immediate risk of harm [...], suicidal or self-harming



Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS – search.gov.uk

"We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!"



It is important that everyone understands that whilst sexting is illegal, pupils 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 nudes.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils 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. Please refer to Cranbrook Primary's Anti-bullying Policy.

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

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

Child-on-child sexual violence and harassment

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

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 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.

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/handbook

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

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

The responsibilities for filtering and monitoring, led by the DSL and following DfE standards, may mean that more such incidents will be discovered in the coming year but the school will do its best to remind pupils and staff of this increased scrutiny.

Social media incidents

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

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

CCTV

We have CCTV in the school as part of our site surveillance for staff, pupil and property safety. We will not reveal any recordings without appropriate permission.

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 cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found on the [school website](#).

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, and Meraki Mobile Device.

Cranbrook Primary School use Impero/Senso as an additional safeguard layer in protecting children and staff. The software monitors all computers/laptops and sends alerts in the case of possible 'incidents' or key word violations.

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

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with the IT Team 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 look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

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 email 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 check and also to ensure that the school responds to issues and integrates with the curriculum.

We carry out 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.

Safe Search is enforced on any accessible search engines on all devices. Our YouTube mode is Moderate restricted.

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.

The DSL checks filtering reports and notifications and takes any necessary action as a result. According to the DfE standards, “a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

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

At Cranbrook Primary School we use all three options.

At home, school devices are protected with Sophos and LGfL HomeProtect.

When pupils log into any school system on a personal device, activity may also be monitored here.

At Cranbrook Primary School:

- web filtering is provided by LGfL on school site and for school devices used in the home
- changes can be made by the IT Team.
- overall responsibility is held by the DSL
- technical support and advice, setup and configuration are from the IT team.
- regular checks are made half termly, by the IT team, to ensure filtering is still active and functioning everywhere.
- guidance on how the system is ‘appropriate’ is available at appropriate.lgfl.net

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

- Pupils at this school use the LondonMail / PupilMail system from LGfL and Microsoft Outlook within Office 365 for all school emails (if required)
- Staff at this school use the StaffMail system for all school emails, Microsoft Outlook within Office 365 and the London Borough of Redbridge service.

These systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. Redbridge emails are managed by the London Borough of Redbridge. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email and Microsoft Teams are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance. 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).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
 - If data needs to be shared with external agencies, Egress system is available from LGfL.
 - Internally, staff must use the school network. When working from home, staff must use the remote access which is available via the RAV3 system (freedom2roam) or Terminal Server or school-run Office365 or LGfL MyDrive.
 - Staff must use Egress when sharing sensitive information with outside agencies
- Pupils at the school are restricted to emailing within the school and cannot email external accounts.
- 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
- 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.

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 this 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.

Use of generative AI

At Cranbrook Primary School, we acknowledge that generative AI platforms (e.g. ChatGPT or Bard 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, deepfakes, undressing apps).
- The use of any generative AI to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.

Online storage and 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 cyber security before adopting such a platform or service and at all times when using it.

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 DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at safepolicies.lgfl.net to help schools to ensure that requirements are met (see appendices).

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

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of high quality public-domain images that can be used. Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

Online storage or learning platforms

It is important to consider data protection before adopting a cloud platform or service – see our DP policy [here](#). At Cranbrook Primary we use Microsoft's Office 365, LGfL myDrive for file storage setting homework and distributing reports etc.

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

and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

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

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

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 Cranbrook Primary School, no member of staff will ever use their personal phone to capture

photos or videos of pupils. Should the need arise (in emergencies only) members of staff may 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 – This includes a where phones automatically back up photos).

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

Staff and parents are reminded annually (at minimum) 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. Further detail on this subject and a sample letter to parents for taking photos or videos at school events can be found at parentfilming.lgfl.net

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

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

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

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

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

Many social media platforms have a minimum age of 13, (note that WhatsApp is 16+). However, on occasions, the school deals with issues arising on social media with 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 that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils 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). Please refer to the [Top Tips for Parents](#) poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

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

Staff/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). 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, and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the headteacher (if by a staff member).

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 6 years, there have been 333 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

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.

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

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

- **Pupils/students** in Year 6 may be allowed to bring mobile phones to school with the written permission from parents/carers (usually for children who travel to and/or from home on their own). However, phones **MUST** be left at the school office at the start of the day and must be collected at the end of the school day. Pupils are not allowed to wear smart watches with cameras within CPS.
- **All staff who work directly with children** should leave their mobile phones in a secure location on silent and only use them in an area away from the school or just outside the school office. Child/staff data should never be downloaded onto a private phone. If a staff member is

expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office. Any smart watch with a camera should be left in a secure place. It shouldn't be used within the school premises. Staff are not allowed to wear smart watches with cameras within CPS.

- **Volunteers, contractors, governors and visitors** 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. Any smart watch with a camera should be left in a secure place. It shouldn't be used within the school premises. **Volunteers, contractors, governors and visitors** are not allowed to wear smart watches with cameras within CPS.
- **Parents** – where parents are regularly in the playground for drop-off or collection. Cranbrook Primary will continuously encourage or ask parents/carers to leave their phones in their pockets and remind parents about turning them 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. When at school events, parents are asked not to use their mobile phones on the school premises. We encourage 'Greet your child with a smile NOT a mobile'. Parents should avoid the use of smart watches (with a camera) on school grounds.

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.

Wi-Fi is accessible to staff/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.

Network / internet access on school devices

- **School devices** are issued to some students. These are restricted to the apps/software installed by the school and may be used for learning and reasonable as well as appropriate personal use at home but all usage may be tracked. The devices are protected by Sophos and LGFI HomeProtect.
- **All staff who work directly with children** should leave their mobile phones in a secure location on silent and only use them in an area away from the school or just outside the school office. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, staff will have their mobiles phones with them and only use them when contacting the school or any other emergency situation. 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 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.

Searching children suspected of having prohibited items

If it is suspected that a child has brought a serious prohibited item into the school the child will be asked to hand over to a senior member of staff, in the presence of an additional member of staff as a witness. The child will be asked for permission to search their coat, bags etc., if they are not willing to hand over the items. Should they refuse the Head reserves the right to search their bag without consent, an additional adult should always be present.

If it is suspected that the child is carrying prohibited items about their person and refuses to hand them over, the school reserves the right to use reasonable force whilst a search takes place. If they are suspected of carrying a weapon or illegal items then the police will be notified.

Appendix A- Acceptable Use Policies

1. Acceptable Use Policies (AUPs) for:
 - *Pupils (EYFS / KS1 and/ KS2)

- *Staff, governors and volunteers
- *Visitors and contractors

Appendix B – 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

Key responsibilities:

- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment
- Recognise that **RSHE** is statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject.
- Understand that online safety is a core part of safeguarding; as such it is part of everyone’s job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and who is also the Online Safety Lead (OSL)

- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures (CPOMS).
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook (sent via SchoolPing).
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE/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).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework or remote teaching tasks, encourage sensible use, monitor what pupils are doing, talk about appropriate behaviour, 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).

- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Know how to report this through the internal school channels
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to all forms of bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of

the school and of the professional reputation of all staff. More guidance on this point can be found in this [Online Reputation](#) guidance for schools.

Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL- if needed. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Headteacher – Cassim Bana

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 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 –Kimberly McKoy

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 – translations are available in 13 community languages at kcsietranslate.lgfl.net (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.
- Ensure that 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 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.
- Receive regular updates about 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.

Governing Body, led by Online Safety / Safeguarding Link Governor – Debbie Wiles

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 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.

PSHE/RSHE Lead – [Khaium Miah/Samantha Patel]

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/RSHE 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.”
This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- 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.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within RSHE. Note that an RSHE policy should now 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 – Khaium Miah

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 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/Technician

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.
- 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 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.

Data Protection Officer (DPO) – David Powell

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security 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. You should check the requirements in your area.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

LGfL TRUSTnet Nominated contacts –

Key responsibilities:

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering and monitoring settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL at gdpr.lgfl.net

Volunteers and contractors (including online tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Cranbrook Primary does not use volunteer/contract online tutors.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

External groups including parent associations – CFA

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

DRAFT