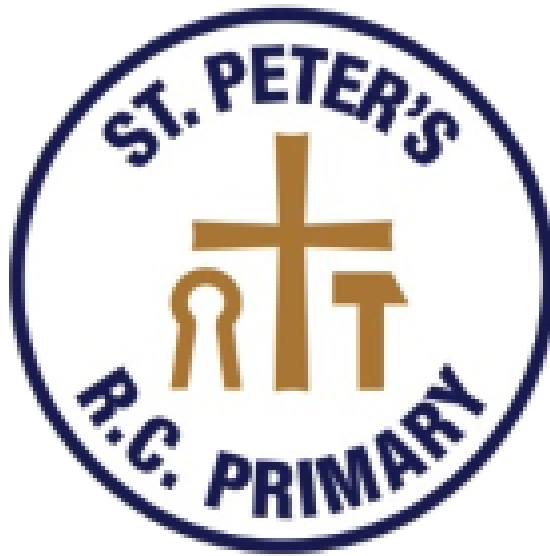


St Peter's R.C. Primary School

Online Safety Policy



Policy	Online Safety Policy
Date	November 2025
Date of review	November 2026
Chair of Governors	<i>Rachel Mahon</i>
Headteacher	<i>C. Scott</i>

Mission Statement

*We, the family of St Peter's, united by our faith by God,
love, learn and grow together.*

Introduction

Key people / dates:

St Peter's Catholic Primary School  The logo of St Peter's R.C. Primary School is a circular emblem. It features a blue outer ring with the text 'ST. PETER'S' at the top and 'R.C. PRIMARY' at the bottom. Inside the ring is a gold cross with a stylized figure of a person standing in front of it.	Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Mrs Clare Scott
	Deputy Designated Safeguarding Leads / DSL Team Members	Ms Rebecca Anthony Ms Stephanie Doe Miss Eva Rauch
	Link governor for safeguarding and Web filtering	Mrs Carmel Casey
	Curriculum leads with relevance to online safeguarding and their role	Mr L Maguire Computing Lead
	Network manager / other technical support	Edunet ICT
	Date this policy was reviewed and by whom	Reviewed by Miss Anthonney – November 2025
	Date of next review and by whom	Updated as required Full review November 2026

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2024 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and sits alongside the school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety will follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and is possible to follow in all respects. This will help all stakeholders to understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies for different stakeholders help with this – school will ensure these are reviewed alongside this overarching policy. Any changes to this policy will 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 and understanding the filtering and monitoring systems and processes in place)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

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

Current Online Safeguarding Trends

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

	Solutions to mitigate the risks
Identified Risky Behaviours	At Home
Children accessing the online world without any/adequate supervision: many children, especially in KS2 but increasingly across all age groups, report using devices online without an adult present, especially in their own bedrooms.	Ensure children are supervised at all times when online and discuss with them what it is they do/access when online – part of the children's learning we teach in school is about always telling the adults at home what you are doing when online, so talk to them about this and set your own expectations at home.

Children accessing inappropriate online content, especially: age inappropriate video clips (especially horror or scary clips), music with inappropriate content (especially language and/or sexualised behaviours), age inappropriate online gaming, age inappropriate language (especially swearing) sexually inappropriate language and video content.	If suitable restrictions and supervision are in place, this considerably mitigates this risk, but it is also worth having conversations with your children about what content is appropriate/inappropriate and what to do if they encounter something that is inappropriate, makes them feel worried or unsafe – children share that the main reason for not informing adults at home what they do online, is fear of having devices taken away, so open, honest dialogue and developing a shared understanding of what is appropriate or not is vital.
--	---

Children posting messages and/or photos and/or videos of themselves online.	School would encourage children to not post online content, especially photos and videos of themselves. However, we recognise that children are increasingly interested in this area. We encourage families to discuss with their child whether posting online is appropriate and desirable in the first place. If so, ensure any platform/forum used is age appropriate and ensure any privacy settings are enabled to ensure content is only shared with known and trusted contacts. Discuss the fact that once content is posted it can be used by others in ways they did not originally intend and/or others might comment on their content in ways they might not like.
Children communicating with strangers online Children joining online groups (often through gaming) that include strangers.	Ensure you know what systems/games children use to communicate with others and only let them do so with people they actually know and trust (i.e. have met in the physical world)
Children sending one another abusive messages through social media/online message forums (i.e. cyber bullying)	Discuss with children: how to behave; how inappropriate behaviours would make them/others feel; and online reputations and how things that are posted online can be seen by many and potentially forever.
Children having unrestricted access to the online world, especially: YouTube, social media and online gaming	Find out about ways to restrict children's online access, including the use of safety settings on devices. Talk to children about what they want to access and why and ensure it is age appropriate and does not put them at risk of inappropriate content being accidentally viewed. View content with or before your child, to ensure it is

	appropriate.(Note that many social media and digital platforms use algorithms to drive content towards the end user and these can lead to undesirable suggestions being shown.)
The impact of extended screen time on general wellbeing.	Find out about ways to reduce screen time, including setting limits on all devices

At school, in addition to what we do to mitigate these individual risks, we also do the following:

- Treat each and every online safety incident as a Safeguarding issue and record and manage the response in line with our safeguarding policy. Staff use any incidents as an opportunity to talk to children and understand how and why situations have arisen. We then support and educate children, as well as families, about how to behave safely and appropriately when online.
- Cover the full range of online safety learning through both our PSHE and Computing curricular, to ensure full and thorough coverage. Year groups will cover online safety in the following ways, throughout the year:
 1. **Teach** - Cover an element of the online safety curriculum at least every half term.
 2. **Follow up** – We will cover online safety for Years 1-6 in assemblies at different points during the year. Teachers will have follow up conversations in class with children to reinforce this learning.
 3. **Reinforce** – Throughout the year when teaching other subject content, staff will **actively seek opportunities for reinforcing online safety learning** that is relevant (e.g. when researching online, make explicit links to managing information online and differentiating between opinion, belief and facts; or when looking at relationships and communicating with other, discussing the relevance of this in both the physical and online worlds)
 4. **Respond** – As part of their everyday roles, staff monitor children's behaviours

And conversations to look for signs of anything concerning or inappropriate. If an online incident occurs, or staff notice some unhealthy or concerning online behaviours or attitudes, these are used as a learning opportunity to help remind/teach children about the relevant online safety topic (e.g. A conversation comes up about sharing passwords)

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 4Cs (see below), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising or phishing. Public Health England: has now been replaced by the UK Health Security Agency and the Office for Health Improvement and Disparities (OHID), which is part of the Department of Health and SocialCare, and by the UK Health Security Agency, however branding remains unchanged.

Self-generative artificial intelligence has become rapidly more accessible, with many students often having 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 (gen AI can be responsible for incorrect and sometime harmful 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. Self-generative AI has also made it easier than ever to create sexualised images and deepfake videos. Whilst they may not be real, they have a devastating effect on a young person's emotional wellbeing and physical safety, and can also be used to blackmail, humiliate and abuse. The Internet Watch Foundation has reported AI-generated imagery of child sexual abuse progressing at such a worrying rate.

Ofcom's 'Children and parents: media use and attitudes report 2024' has shown that

YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, Tok-tok and Snapchat increased yet further (especially with the minimum age for use of WhatsApp now 13). With children aged 3 - 17 spending an average 3 hours 5 minutes per day online, four in ten parents report finding it hard to control their child's screentime. Notably, 45% of 8-11s feel that their parents' screentime is too high, underlining the importance of modelling good behavior. Given the 13+ minimum age requirement on most social media platforms, it is notable that half (51%) of children under 13 use them. 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 (36%) 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 pupils 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.

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

Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 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.

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
- Available in paper format in the staffroom
- Part of school induction (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers
- Discussed in parent workshops

Overview

Aims

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

- Setting out expectations for all St Peter's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective

collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RHE) and beyond.

- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day,

regardless of device or platform, and that the same standards of behaviour apply online and offline.

- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
 - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online incidents 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)

Scope

This policy applies to all members of the St Peter's 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. All staff have a key role to play in feeding back on potential issues.

Education and curriculum

Despite the risks associated with being online, St Peter's Catholic 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 [through] tests, written assignments or self-evaluations, to capture progress.” The teaching of online safety, features in these particular areas of curriculum delivery:

- Relationships and health education (RHE) (also known as PSHE)
- Computing
- Citizenship

However, as stated previously, 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. Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme- based resources, materials and signposting for teachers and parents.

At St Peter’s Catholic Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we adopt the cross-curricular framework following the Purple Mash and Project Evolve schemes of work. Annual reviews of curriculum plans / schemes of work (including for SEND pupils) take place and are used as an opportunity to follow this framework more closely in its key areas. This is done within the context of an annual online safety audit, which is a collaborative effort led by Mrs Clare School – DSL and Mr L Maguire-Computing Lead.

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 by sharing this policy, sharing the curriculum, updates in newsletters and during the online safety workshop with parents.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the safeguarding lead with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom. 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
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy
- Cyber Security Policy
- CCTV Policy

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

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

Any concern/allegation about staff misuse is always (similar to any safeguarding concern) referred directly to the DSL/Headteacher, unless the concern is about the DSL/Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer- Mike Cullern). Staff may also use the NSPCC Whistleblowing Helpline, all contact information available in the staffroom.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance **Behaviour in Schools, advice for headteachers and school staff** September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law. The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

The following sub-sections provide detail on managing particular types of concern:

Nudes – sharing nudes and semi-nudes

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

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

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

The school DSL will 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 (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils. The following LGfL document (available at **nudes.lgfl.net**) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:

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!"

LGfL
SafeguardED

Priority Areas

Upskirting

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

Bullying

Online bullying (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed. This includes issues arising from banter. School understands it is important not to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline elements. It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment

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

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 found on the school website 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 or the Safeguarding policy.

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.

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

Social media incidents

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

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/Safeguarding policy (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults in the St Peter's community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), St Peter's 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

CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance at the school is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;

- promoting the health and safety of staff, pupils and visitors as well as for monitoring student behaviour;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

The system does not have sound recording capability. The CCTV system is owned and operated by the School, the deployment of which is determined by the School's leadership team.

The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the school community. The School's CCTV is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images.

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 and cyber security policy which can be found on the school website. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges. Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The designated safeguarding lead (DSL), Mrs Scott, has lead responsibility for filtering and monitoring and works closely with Mr L Howe 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.

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 half-termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc. More details of both documents and results are available on request dependent on staff roles from the DSL Mrs Scott.

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 by reporting to the DSL and will be asked for feedback at the time of the regular checks which will now take place.

Safe Search is enforced on any accessible search engines on all devices. Our YouTube mode is moderate restricted with DNS restrictions on. Out of hours, our policies remain the same.

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 monthly 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 at St Peter’s these 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

We look to provide ‘appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times and at St Peter’s Catholic Primary School:

- Web filtering is provided by LGfL
- Any school devices provided for home use will also be installed with an appropriate web filter
- Overall responsibility is held by the DSL, with support from the Computing Lead
- Technical support and advice, setup and configuration are from Edunet
- Regular checks are made half termly by DSL Mrs Scott or Mr Maguire - Computing Lead to ensure filtering is still active and functioning everywhere. These are evidenced on the filtering and monitoring check-list and discussed with the SLT/Safeguarding Team
- An annual review is carried out as part of the online safety audit to ensure a whole school approach
- Guidance on how the system is ‘appropriate’ is available at appropriate.lgfl.net

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

Authorised systems

- Pupils at this school can communicate with each other using Google Classroom, through posts initiated by the classroom staff on the main newsfeed. They cannot initiate these posts. They are also able to communicate with classroom staff, through the assignment commentary function. This is monitored closely by classroom staff and, if required, staff can request that pupils have their ability to do this removed.

- Staff at this school use the email system provided by LBBD 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 relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with parents, colleagues, or with external organisations or agencies, but not with under 18s.

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

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If 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.

Behaviour / usage principles of messaging/commenting systems

- 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 the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy, available on the school website and only using the authorised systems mentioned above.

Use of generative AI

At St Peter's, 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 in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.

- In school, we take a risk-based approach. We currently block generative AI on the filtering system for pupils and if/when appropriate we may choose to allow generative AI on a one- by-one basis for those sites/apps we deem to be acceptable/required, with limitations according to age and/or for certain lessons or periods of time.
- With regard to staff use of generative AI, we allow its use to support resource development such as images or diagrams which support the teaching and learning of specific content. For example, creating plot point images for narrative maps in writing lessons. Staff will be provided with relevant training to ensure effective and accurate use of generative AI to support in their roles.
- AI platforms will be approved by the senior leadership team after extensive risk management process which will include research and discussion regarding the potential needs versus the potential dangers.

Online storage or learning platforms

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

St Peter's R.C. Primary School utilises the suite provided by Google for Education, which has transparent data protection, and cybersecurity policies and practice. In addition, the school has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times. 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. Any new platforms will be approved by Mrs C Scott-Headteacher.

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 the school computing and technical staff team.

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

Digital images and video

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

- For displays around the school

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

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 St Peter's Catholic Primary School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school's local network in line with the retention schedule of the school Data Protection Policy. Mrs Scott and Mr Maguire carry out termly checks of images/video on school devices. Any concerns about the nature of these images will be reported to the DSL.

Staff and parents are reminded regularly, at least termly and during all school events, about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children. Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

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

Social media

Our SM presence

St Peter's works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online. Negative coverage almost always causes some level of disruption. 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. The Computing/ Technical staff team, alongside the senior leadership team are responsible for managing our X-Twitter social media accounts and checking our Wikipedia and Google reviews and other mentions online.

Staff, pupils' and parents' SM presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policy, 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 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, found on the school website, should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 but the school regularly deals with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise.

Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the [Digital Family Agreement](#) to help establish shared expectations and the [Top Tips for Parents](#) poster along with relevant items and support available from parentsafe.lgfl.net and introduce the [Children's Commission Digital 5 A Day](#).

Although the school has an official X-Twitter account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school alongside Groupcall for communicating with parents in the form of message notifications to their mobile devices. Social media, including chat apps such as WhatsApp, are not appropriate for school use. As outlined in the Acceptable Use Policies, 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, however, staff must not follow such public pupil accounts. 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).

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).

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, or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Device usage

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

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

- **Smart watches or other wearable devices are not permitted for pupils to use in school, unless permission has been granted by the Headteacher e.g for medical monitoring purposes.**
- **Pupils in Year 6** are allowed to bring mobile phones in for emergency use only. During the school day, phones must remain turned off at all times and are handed in to the class teacher. Any attempt to use a phone in school time or to take illicit photographs or videos will lead to sanctions in line with the behaviour policy, as well as the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. Our approach to pupils using mobile phones is in line with DfE, Mobile Phone Guidance.
- **All staff who work directly with children** should leave their mobile phones on silent and out of sight when working directly with pupils and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cyber security policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on

duty, they must seek permission from the senior leadership team first.

- **All staff who work directly with children** should leave any smart watch or wearable device in school or airplane mode during all contact time with children.
- **Volunteers, contractors, governors** should leave their phones in a bag 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 encouraged to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Please see the Digital images and video section of this document for more information about filming and photography at school events. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
- Where BYOD is allowed, neither staff nor students are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home. School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wi-Fi is accessible to staff and pupils for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

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

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number 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 that the number is hidden to avoid a parent or student accessing a teacher's private phone number. Groupcall is used for all communication between school and parents in the form of text message alerts. This will be used to keep parents informed about trips, updates and emergency communications.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools](#)', the Headteacher Mrs C Scott, Deputy Headteacher Ms R Anthoney 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. Full details of the school's search procedures are available in the school Behaviour Policy, available on the school website.

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

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

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

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

Headteacher Mrs C Scott

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 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 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 – Mrs Scott

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. RHE), 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 [

dedicated resources at parentsafe.lgfl.net.

- Communicate regularly with SLT and the safeguarding governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.

- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine, 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 AUP, and those hired by parents. [share [the Online Tutors – Keeping Children Safe](#) poster at parentsafe.lgfl.net to remind parents of key safeguarding principles].

Safeguarding / Web Filtering Link Governor – Mrs Casey

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.
- Work closely with the DSL on the new filtering and monitoring standards [there is guidance for governors at safefiltering.lgfl.net].
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring).
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology.”

PSHE / RHE Lead- Mr Sullivan

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 latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."
- Focus on the underpinning knowledge and behaviours outlined in **Teaching Online Safety in Schools** in an age-appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self-evaluations, to capture progress" - to complement the computing curriculum,.
- Work closely with other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Lead – Mr Maguire

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 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.

Network Manager- Edunet

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.

- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards, protections for pupils in the home and remote-learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to pupils and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – Data Protection Enterprise Ltd
DPO@st-peter.bardaglea.org.uk

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.

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session**, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental code of conduct including the schools acceptable use policy.

External groups (e.g. those hiring the premises) including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school. staff, volunteers, governors, contractors, pupils or other parents/carers.

