SURREY COUNTY COUNCIL
DIOCESE OF ARUNDEL AND BRIGHTON

St. Peter's Catholic Primary School

Online-Safety Policy

Based on LGFL model policy

Agreed by Governing Body in June 2019
Reviewed in September 2024
Next Review September 2025

Headteacher: Lisa Kelly
Online-safety Lead: Ruth Hall
Responsible member of the Governing Body: Laura Jackson
Designated Safeguarding Lead: Ruth Hall
Deputy DSLs: Lisa Kelly, Amanda Walsh Barbara Tucker and Alex McWilliams

UK SAFER INTERNET CENTRE HELPLINE 0844 381 4772

Introduction

Key people / dates

Designated Safeguarding Lead (DSL) team	Lisa Kelly Ruth Hall Amanda Walsh Alex McWilliams Barbara Tucker
Online-safety lead	Ruth Hall
Online-safety / safeguarding link governor	Laura Jackson
PSHE/RSHE lead	Lisa Kelly and Ruth Hall
Network manager / Data protection officer / other technical support	Ethna Clegg / Tom Devaney Soft Egg Limited
Date this policy was reviewed and by whom	September 2024 Lisa Kelly Ruth Hall
Date of next review and by whom	September 2025 Lisa Kelly Ruth Hall

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory Relationships, Sex and Health Education (RSHE) guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing.

Who is in charge of online safety?

Ruth Hall is the designated online safety lead but **KCSIE makes clear that "the designated safeguarding lead (Ruth Hall) takes lead responsibility for safeguarding and child protection (including online safety)."**

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2024, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, 'upskirting' and sticky design.

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 on the internal staff network/drive
- Available in paper format on request from Designated Safeguarding Lead or Online Safety Lead
- Part of school induction pack for all new staff (including temporary, and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff and pupils (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
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Contents

Overview

Aims

This policy aims to:

- Set out expectations for all St Peter's Catholic Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- 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
- 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
    - 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 your 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). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, **Surrey CC** 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.

Scope

This policy applies to all members of the St Peter's Catholic Primary School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, 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.

Headteacher/Principal – Lisa Kelly

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- 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
- 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 GDPR-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
- 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 cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- 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 that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements.
- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards.

Designated Safeguarding Lead / Online Safety Lead – Ruth Hall

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2023):

- "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)."
- Work with the HT and technical staff to review protections for **pupils in the home** [Securly Filtering] and **remote-learning** procedures, rules and safeguards.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Ensure "that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- 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 with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends

- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety 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/lockdown, e.g. a safe, simple, online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are also aware. Make key decisions on what should be allowed and ensure communication with technical teams to make sure it is in place. Ensure that the priority is to keep children safe and "that appropriate filtering and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding." (KCSIE 2024)
- Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
    - all staff must read KCSIE Part 1 and all those working with children Annex B – translations are available in 12 community languages at kcsietranslate.lgfl.net
    - Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
    - it would also be advisable for all staff to be aware of Annex D (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
- 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.

Governing Body, led by Online Safety / Safeguarding Link Governor – Cath Woolford

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2024)

- 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
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards (see remotesafe.lgfl.net for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- "Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. 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)." and "should ensure the designated safeguarding lead has the appropriate status and authority within the school or college to carry out the duties of the post. The role carries a significant level of responsibility and the postholder should be given the additional time, funding, training, resources, and support needed to carry out the role effectively."
- 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.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Work with the DPO, DSL and headteacher to ensure a GDPR-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; check that Annex D on Online Safety reflects practice in our school.
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach."
- "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." This includes St. Peter's approach to adopting the UKCIS cross-curricular framework 'Education for a Connected World – 2020 edition' to support a whole-school approach

All staff

Key responsibilities:

- Recognise that **RSHE** is now 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 Online Safety Lead (OSL) are.
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections). Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- 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.
- 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. See appendices
- 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 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 in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place).
- When supporting pupils remotely, be mindful of additional safeguarding considerations
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and 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
- Encourage pupils/students 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 sexual harassment (your DSL will disseminate relevant information from the updated 2021 DfE document on this).
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to 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.

PSHE / RSHE Lead/s – Lisa Kelly and Ruth Hall

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe 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."
- 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.
- Work closely with the DSL / OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / 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 / Deputy – Kathryn Scott / Guy Barlow

Key responsibilities:

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

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

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Embed the aims of the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools via Project Evolve in Computing lessons in Autumn Term of each year.
- 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 – Ethna Clegg / Soft Egg

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for **pupils in the home** [Securly Filtering] and **remote-learning** procedures, rules and safeguards.
- 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.
- Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that school systems and networks reflect school policy.
- 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.).
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team.
- 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.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – Tom Devaney

Key responsibilities:

- NB – this document is not for general data-protection guidance.
- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (updated August 2023), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule 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.

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

IT Contractors - Soft Egg Limited

Key responsibilities:

- To ensure all IT services are managed on behalf of the school in line with school policies, following data handling procedures as relevant.

- Work closely with the OSL, DPO and Network Manager 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.

Volunteers and contractors (including tutors)

Key responsibilities:

- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator.
- 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.
- Tutors contracted by the school will be required to sign the staff AUP.
- Note that as per AUP agreement a tutor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, and adhere to the student/pupil acceptable use policy and review this annually.
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen.
- 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.
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.

- 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.

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use of social media policy and read and sign the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and 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.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

External groups including parent associations – FOSP

Key responsibilities:

- 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.

Education and curriculum

At St Peter's Catholic Primary School, we recognise that online safety and broader digital resilience must be threaded 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).

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.

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 online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

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

School procedures for dealing with online-safety 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
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

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

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

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline

The school will actively seek support from other agencies as needed (i.e. SCC, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). 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 and upskirting; see section below).

Sexting – sharing nudes and semi-nudes

St Peter's Catholic Primary School 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 to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview 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.

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.

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/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 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. See Anti-Bullying Policy.

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

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. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

The rules and procedures are clearly defined in the relevant Acceptable Use Policies as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

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

It will be necessary remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

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

Social media incidents

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

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, St Peter's Catholic 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.

Data protection and data security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

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

- We follow LA guidelines for the transfer of any data.
- We require that all staff laptops are encrypted with Bitlocker for when the devices are removed from the school.
- We have a remote access solution so staff can access sensitive data from home without the need to take data home.
- We require staff to sleep their computers when they leave them at the end of the day, but also enforce a lock out after idle time.
- We use DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Surrey Admissions System to transfer admissions data.
- All servers are in secure locations and managed by DBS checked staff.
- Our back up is offsite and held by Soft Egg.
- We use CPOMS to transfer child protection data internally and to external agencies.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided by Soft Egg. This means we have a dedicated and secure, connection that is protected with firewalls and multiple layers of security, including a web filtering system called Securly, which is made specifically to protect children in schools.

At home, school devices are filtered and monitored when on home wifi connections.

When pupils log into any school system on a personal device, activity may also be monitored here. For example, if a pupil logs onto their school G Suite account they will monitored and restricted as per the domain settings.

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

This school uses the following

- Pupils at this school use the GMail system for all school emails
- Staff at this school use the Office 365 system or their school Gmail for all school emails

Both these systems are fully auditable. 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 is 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. For instances of Home learning the headteacher has approved the use of the school's G Suite as means of communication (e.g. Google classroom and Meets for staff and pupils), but his is not to be used by parents. This approval will be periodically reviewed as needed. 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. We use secure LA/DFE approved systems, see Data Management.
- Pupils in KS2 are restricted to emailing within the school's whitelist and cannot email external. The whitelist is reviewed annually to allow for the addition and removal of JDO partner schools.
- 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
- Pupils and staff are NOT allowed to use the email system for personal use and 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.

See also the social media section of this policy.

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 to Ruth Hall. The DfE has determined information which must be available on a school website and it is their responsibility to ensure this is up to date and compliant.

The site is managed by / hosted by E4Education.

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.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

St Peter's has adopted G Suite for Education as its cloud platform.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud.
- 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.
- 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/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 displays and assessment, which does not require express consent). Parents answer as follows:

We ask parental permission to share images/ videos in the following ways:

1) In school publications e.g. newsletters/ prospectus etc. PLEASE NOTE this also includes website permission

IT IS IMPORTANT THAT PARENTS NOTE THAT OUR PRINT AND DIGITAL PUBLICATIONS ARE THE SAME AND THE WAY THAT OUR SCHOOL WORKS MEANS THAT IT IS NOT POSSIBLE TO GIVE PERMISSION FOR ONE WITHOUT THE OTHER.

2) In videos which appear on the school Vimeo channel and on the school website

The benefits of the use of video have been proven to be so valuable in sharing the wonderful work of our school, especially during recent Covid-19 restrictions. When we have not been able to invite parents into school events (e.g. our nativity plays, carol concerts, Mass, leavers productions etc.), we have been able to video them and share them with parents. We occasionally make video tours to explain our approaches, which are then made available on our school website and Vimeo channel.

Please note that non speaking photo montage videos are covered under the 'image' permission. Videos will be hosted on the school website and Vimeo channel but WILL NOT be downloadable without a password given to parents.

3) In training events for other teaching professionals

We may use images of children at work in their learning environments in slideshows and hand-outs used during training events or to illustrate articles written.

4) On our school Facebook page

The use of pictures or videos on the school Facebook page would be for extraordinary events only and is most likely to be in the style of a whole school video montage e.g. the Euro 2021 song. When we share pictures/ videos on the Facebook page NO NAMES will be used.

5) In local newspapers e.g. for leavers supplements or coverage of local events

Parents should be aware that with the exception of the First Days at school supplement and large group or team photographs is likely that media organisations would wish to publish the child's name, age and the school's name in the caption for the picture.

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 network or the school Google Drive in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded at whole school events about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

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

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

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

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

Social media

St Peter's Catholic Primary School's SM presence

It is important to us that families of our children can find the information that they need about St Peter's easily. St Peter's Catholic Primary School recognises the power that social media has to connect parents and build communities.

Ruth Hall is responsible for managing our Facebook account. She follows the guidance in the LGfL / Safer Internet Centre online-reputation management document here.

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+), but the school occasionally deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use.

The school has an official Facebook account (managed by Ruth Hall) and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

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

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

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

Staff that are also parents are strongly advised to not join parent 'WhatsApp' groups. If they do they must not engage in discussions re school issues and staff are reminded that joining such a group will expose their private number to the entire group.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).

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

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 263 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 (see page) 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

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

Personal mobile phones and mobile devices

Staff

- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- During emergency lock-down practices and actual incidents, staff are told to keep their phones and laptops with them in order that a channel of communication can be maintained.

Staff / Visitor use of personal devices

- Staff may bring mobile phones into school. These should routinely switched off while in the classroom and only used in staff areas during break, lunchtimes or during release time from class. However, in the following situations, the use of personal mobile phones is allowed*:

- Staff who are dealing with challenging behaviour, for example, supervising a child outside the classroom are encouraged to keep their mobile phone with them, so that they can call the school office should they require further assistance.
- If a member of staff has exceptional circumstances where they feel that they need their mobile phone with them (awaiting call from doctor etc). They must leave the classroom, with appropriate supervision in place, to take any calls.
- If staff need to contact the IT provider, Soft Egg for remote access support. This typically needs to be done in the vicinity of the device which is experiencing issues.

*it should be noted that in these circumstances, phones should be out of site e.g. a pocket when not in use and not used in the corridor/ pupil areas except in an emergency.

- If members of staff have an educational reason to allow children to use mobile phones or a personally owned device as part of an educational activity then it will only take place when approved by the SLT
- Staff should never use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes
- If a member of staff breaches the school policy then disciplinary action may be taken.

Visitors and Contractors

- All visitors including parent volunteers/ helpers are requested to keep their phones on silent and out of reach. Parent helpers are also advised that that they are not allowed to use mobile phones or devices to take photographs unless specifically agreed by the SLT

Pupils

Pupils' use of personal devices

Our school strongly advises that pupils do not bring mobile phones into school but accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. In order to balance the need for children to feel safe when offsite with our safeguarding responsibility we:

- Publish a Mobile Phone agreement which is only applicable to children who walk to and from school in Year 5 and6 and which all children and parents must sign before they are permitted to bring a mobile phone on site.
- Mobile phones will be handed to the class teacher and stored in safe-keeping during the day. If a child needs to contact his or her parents or carers, this will be managed by the school office
- If a child breaches the agreement, then the phone will be confiscated and will be held in a secure place in the school office and only released to parents or carers.

- Do not allow any other pupils to bring mobile phones into school.
- If children from any year group are found to have any other mobile devices in their possession, they will be confiscated and returned to them at the end of the school day.
- The use of internet enabled devices and/ or mobile phones will not normally be allowed on school trips. The decision whether to allow children to bring an electronic device on a trip will be made by the member of staff leading it.

Network / internet access on school devices

- **Pupils/students** are not allowed networked file access via personal devices or access to the school wifi connection.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours (apart from in certain circumstances – see above). See also the Digital images and video section on page 23 and Data protection and data security section on page 19. Child/staff data should never be downloaded onto a private phone. Any mobile phone connected to the school wifi network will be filtered at the strictest setting.
- **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 and BYOD are subject to the strictest network filtering.
- **Parents** have no access to the school network or wireless internet on personal devices. The **FOSP** 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 and BYOD are subject to the strictest network filtering.

Trips / events away from school

For school trips/events away from school, teachers will use their personal mobile phones in the event of an emergency. 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.

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

Appendices

1. Acceptable Use Policy / ICT Code of Conduct- Staff
2. Acceptable Use Policy / ICT Code of Conduct- KS1
3. Acceptable Use Policy / ICT Code of Conduct- KS2
4. Acceptable Use Agreement for pupils bringing a mobile phone to school
5. Social Media Parental Agreement
6. Pupil Images Policy
7. Pupil Image Consent Form

Staff Acceptable User Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

General responsibilities:

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
- I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology.
- I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, tablets etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. I will be professional in my communications and actions when using school
- ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's Online Safety policy.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Network access and security:

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses to correspond on school matters.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission is gained from the Headteacher to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be password protected.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

Please sign to say that you have read and understood the above guidance and that:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police. I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

- I understand that I am responsible for my actions in and out of the school.

Staff Name:

Role:

Date signed:

Pupil Image Consent Form

Pupil Image Permission - September 2023

We love to share the great work that the children do here at St Peter's.

To ensure that we have the most up to date information about the consent that parents have given for how we use photos and videos of their child, we are asking parents to complete this very short form as soon as possible.

You should complete a separate form for EACH child that you have at St Peter's.

When we are sharing images or video clips, we use generic captions (e.g. Year 4 making masks, or Science Club members), wherever possible. If we use names, we only ever use first names. Children are never identified by their first and last names.

The form asks you to let us know whether you give permission for us to use images/ videos:

- In school publications (newsletters/ prospectus etc)
- On our school website
- In videos which appear on the school Vimeo channel (please note this is for SPEAKING roles)
- On our school Facebook page
- In training events for other teaching professionals
- In local newspapers (e.g. for leavers supplements or coverage of local events)

Please ensure that you have read the Parent Information sheet regarding how we use and share pictures of children at St Peter's before completing the form: http://www.stpeters-leatherhead.co.uk/page/?title=Permission+%26amp%3B+Agreement+Forms&pid=56

You may mix and match permissions as you feel comfortable with. If you would like to amend or withdraw your permission you can do so at any time by emailing Mrs McDonnell deputy@stpeters-leatherhead.surrey.sch.uk

Your email

Child's name *

Child's year group *

School Publications *

Do you give permission for photographs of your child to be featured in school publications (e.g. newsletters or prospectus)?

Yes / No

School Website *

Do you give permission for photographs of your child to be featured on the school website? http://www.stpeters-leatherhead.co.uk/

Yes /No

School Videos *

Do you give permission for your child to appear in video events (e.g the leavers video, our Virtual May Procession, Plays etc). Please note this is for SPEAKING roles as photo montage videos are covered under the 'image' permission. Videos will be hosted on the school website and Vimeo channel but WILL NOT be downloadable.

Yes /No

School Facebook Page *

Do you give permission for photographs of your child to be featured on the school Facebook page (@Stpeters70)?

Yes /No

Training materials *

Do you give permission for photos/videos to be used in training events for other teaching professionals (e.g. pictures of children's work, classroom clips etc)?

Yes /No

Newspapers *

Do you give permission for photographs to appear in local newspapers e.g. leavers supplement or coverage of local events

Yes / No

Anything else?

Is there anything that you would like us to know about using your child's image in school?