



St Paul's CofE (VC) Junior School Online Safety Policy

Promoting, Valuing and Celebrating Achievements in a Christian Setting

'I am the Good Shepherd; I know my sheep and my sheep know me.' John 10:14

Policy Review

Review Cycle	Date of Current Policy	Author(s) of Current Policy	Review Date
Annual	September 2025	David Fingleton	September 2026

Policy Ratification

Role	Name	Signature	Date
Chair of Governors	Albert Owen		
Head Teacher	Caroline Owen		

Details of Policy Updates

Date	Details
01/09/2021	Updated and re-written to reflect new statutory guidance issued in 2021.
08/09/22	Policy review and updates to KCSIE Sept 2022.
25/09/23	Policy review and updates to KCSIE Sept 2023.
02/09/24	Policy review and updates to KCSIE Sept 2024.
10/2/25	Policy review and updates to pupil mobile phones
22/09/25	Policy review and updates to KCSIE Sept 2025.

[Prevent Duty](#): Under section 26 of the Counter-Terrorism and Security Act 2015, we have a duty to prevent people from being drawn into terrorism (Prevent duty). Protecting children from the risk of radicalisation remains part of our school's wider duty to safeguard children and young people. *"Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs."* (KCSIE, September 2016). We are alert to any possible signs which contribute to vulnerability such as family, friends or online influences as well as any changes in behaviour which could indicate a child may be in need of help or protection. We carry out risk assessments of vulnerable children and young people accordingly, work in partnership with other agencies and the family, and ensure staff are suitably trained and supported in keeping with our LSCB procedures."

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 2021 (KCSIE)***, ***Teaching Online Safety in Schools 2019***, updated ***Keeping Children Safe in Education September 2023*** and ***2024*** and statutory ***RSHE*** guidance. It complements existing subjects including Health, Relationships and Sex Education, Citizenship and Computing and sits alongside the school's statutory Safeguarding Policy.

Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Introduction

At St Paul's C of E VC Junior School, we recognise the benefits and opportunities which new technologies offer to teaching and learning. We provide safe and secure internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning.

However, the accessibility and global nature of the internet and associated learning technologies that are available mean that we all need to be aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks safely, independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and the implementation of the relevant policies. In addition to our duty to safeguard staff and learners, we will do all that we can to make our staff and learners 'e-Safe' and to satisfy our wider duty of care.

This policy sets out the ways in which the school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology.
- Build both an infrastructure and culture of Online Safety.
- Work to empower the school community to use the Internet as an essential tool for life-long learning.

What are the main online safety risks?

Online safety risks can be categorised as one of 4Cs: *Content, Contact, Conduct* and *Commerce*. These areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all four. Many of these risks are identified in ***KCSIE***, including sexual exploitation, criminal exploitation, serious youth violence, up skirting and sticky design. The government's investigation into peer-on-peer sexual abuse and Ofsted review highlighted the need for schools to ensure that processes are in place to allow pupils to report sexual harassment and abuse concerns. Key changes within ***KCSIE*** (2025 update) include the incorporation of guidance on addressing misinformation, disinformation, and conspiracy theories. These changes aim to foster a safer digital environment and ensure the integrity of information shared

within our community. At St Paul's C of E VC Junior School, these reports are taken seriously and dealt with swiftly with any concerns being reported through the school's reporting system **My Concern**.

Scope of policy

The Online Safety policy applies to all users, learners, staff and all members of St Paul's C of E VC Junior School who have access to the school ICT systems, both on the premises and remotely. Any user of the school ICT systems must adhere to and sign a copy of the Acceptable Use Policy. The Online Safety Policy applies to all use of computing equipment (fixed and mobile), the internet and all forms of electronic communication such as email, mobile phones and social media.

The school will manage Online Safety as described within this policy and associated safeguarding policies and will inform parents and carers of known incidents of inappropriate behaviour that take place in and out of school.

This policy will be communicated in the following ways:

- Posted on the school website.
- Available on the **All-Staff Documents** policy folder found on SharePoint.
- Available in paper format outside the headteacher's office.
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff).
- Integral to safeguarding updates and training for all staff (especially in refreshers).
- Reflected in the **Acceptable Use Policies** (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers.
- 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.

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Filtering and monitoring logs.
- Surveys/questionnaires of:
 1. Pupils
 2. Parents and Carers
 3. Staff.

Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility

for online safety is held by the Designated Safeguarding Lead, as defined in '**Keeping Children Safe in Education**'.

- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher and senior leaders are responsible for ensuring that the Designated Safeguarding Lead/Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead/Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.
- 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.

Governors

The DfE guidance '**Keeping Children Safe in Education**' states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare this includes ... online safety".

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of 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)"

Governors are responsible for the approval of the **Online Safety Policy** and for reviewing the effectiveness of the policy.

A member of the governing body will take on the role of Online Safety Governor to include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead.
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended).
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the **DfE Filtering and Monitoring Standards**.
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.
- The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

Keeping Children Safe in Education states:

“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). This should be explicit in the role holder’s job description.”

They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”.

They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online”.

The responsibility for online safety is held by the DSL, the school has appointed an Online Safety Lead to work in support of the DSL in carrying out these responsibilities.

DSL:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant governing body meetings/groups.
- Report regularly to headteacher/senior leadership team
- Be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

Online Safety Lead:

- Work closely with the Designated Safeguarding Lead (DSL).
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- Have a leading role in establishing and reviewing the school online safety policies/documents.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners.
- Liaise with technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education: **content, contact, conduct, commerce.**

Curriculum Leads / RSHE Lead

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme – **Project Evolve.**

This will be provided through:

- A discrete programme (***Project Evolve, Be Internet Legends***).
- PHSE and RSHE programmes (***Jigsaw***).
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education 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.”*
- Assemblies and pastoral programme through relevant national initiatives and opportunities (***Safer Internet Day and Anti-bullying week***).

Teaching and Support Staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- They have read, understood, and signed the staff acceptable use policy (***AUP***).
- They immediately report any suspected misuse or problem to Headteacher/DSL for investigation/action, in line with the school safeguarding procedures.
- All digital communications with learners and parents/carers are on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities and implement current policies regarding these devices.
- In lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (***SWGfL Safe Remote Learning Resource***).
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc. (***Sexual Violence and Sexual Harassment in Schools and Colleges DfE 2021***).
- They model safe, responsible, and professional online behaviours in their own use of technology, including **out** of school and in their use of social media.

IT Provider (Praestantia)

The ***‘DfE Filtering and Monitoring Standards’*** says:

“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”

“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”

The IT service provider should have technical responsibility for:

- Maintaining filtering and monitoring systems.
- Providing filtering and monitoring reports.
- Completing actions following concerns or checks to systems.

The IT service provider should work with the senior leadership team and DSL to:

- Procure systems.
- Identify risk.
- Carry out reviews and checks.

The IT Provider is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority.
- There is clear, safe, and managed control of user access to networks and devices.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Headteacher for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated as agreed in school policies.

Learners

- Are responsible for using the school digital technology systems in accordance with the ***Pupil Acceptable Use Policy*** and ***Online Safety Policy***.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school ***Online Safety Policy*** on the school website.
- Providing them with a copy of the ***Pupil Acceptable Use Policy***.
- Publish information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc.
- Parents'/carers' evenings, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to learners in school.
- The safe and responsible use of their children’s personal devices in the school.

Community users

Community users who access school systems as part of the wider school provision will be expected to sign the **Acceptable Use Policy** before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Education and curriculum

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (**RSE**) and health (also known as **RSHE** or **PSHE**).
- Computing.
- Citizenship.

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

Whenever overseeing the use of technology (*devices, the internet, new technology such as augmented reality, etc*) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (*including, extra-curricular, extended school activities if relevant and remote teaching*), supporting them with search skills, critical thinking (*e.g. fake news*), age-appropriate materials and signposting, and legal issues such as copyright and data law.

At St Paul’s C of E VC Junior School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework **Education for a Connected World - UK Council for Internet Safety**.

Annual reviews of curriculum plans / schemes of work (*including for SEND pupils*) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online Relationships, Online Reputation, Online Bullying, Managing Online Information, Health, Wellbeing and Lifestyle, Privacy and Security, and Copyright and Ownership.

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*).

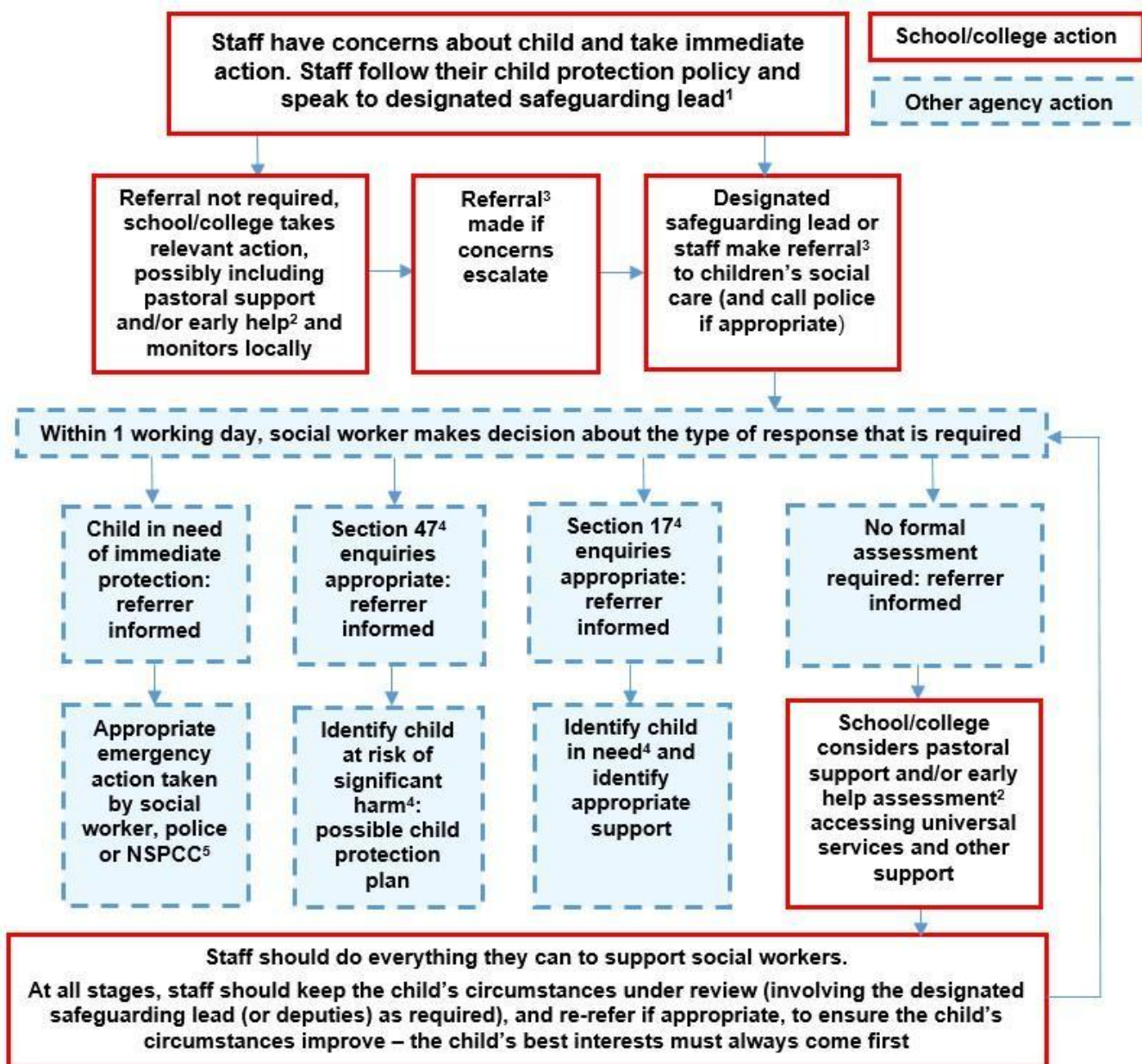
This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (*and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school*). All 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 (*local authority, SWGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), CEOP, Prevent Officer, Police*). 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.

The following flow chart is taken from page 22 of **Keeping Children Safe in Education** as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



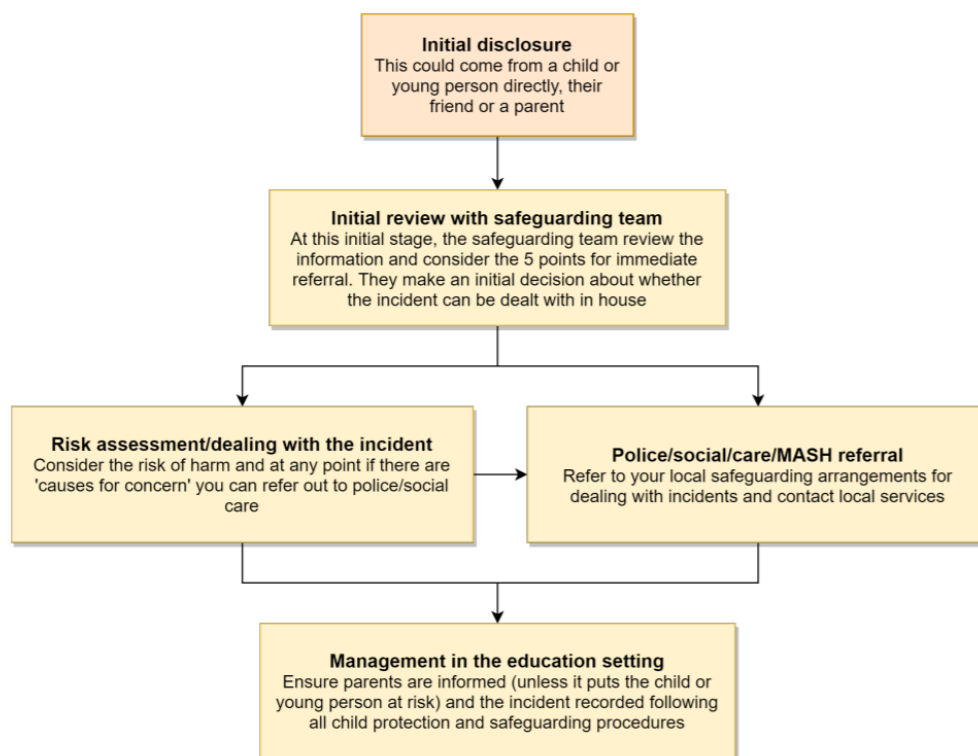
Sexting – sharing nudes and semi-nudes

Incidents of sexting should be immediately reported to the DSL/OSL and reference made 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.

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 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 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 behaviour policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from

banter. It is important to understand that in many cases bullying will often have both online and offline elements.

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in ***Keeping Children Safe in Education*** and a document in its own right.

Any incident of sexual harassment or violence (*online or offline*) should be reported to the DSL who will follow the full guidance. Staff work together to foster a zero-tolerance culture and all forms of sexual violence and harassment are dealt with seriously and not allowed to perpetuate.

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

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

These are defined in the relevant ***Acceptable Use Policy*** as well as in this document.

Where pupils contravene these rules, both inside and outside of school, 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.

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

The rules and expectations of behaviour for children and adults are also governed by the school's ***Acceptable Use Policy***. Breaches will be dealt with in line with the policy.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the 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 ***FOI Policy***, which can be found on the school website.

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 always treated with the strictest confidentiality, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Security

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 **SchoolsBroadband**. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools.

There are three types of appropriate monitoring which are active at St Paul's C of E VC Junior School. These are:

1. Physical monitoring (*adult supervision in the classroom, at all times*).
2. Internet and web access.
3. Active/Pro-active technology monitoring services.

St Paul's C of E VC Junior School will do all that it can to make sure the school ICT network and systems are safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures include the use of filtering and firewalls for servers, routers, and all school provided user devices (*desktop/laptop/tablet/mobile etc.*) to prevent accidental or malicious access of school systems and information.

The school's broadband provider, Schools Broadband, will also complete and update their **Appropriate Monitoring for Schools** document (**UK Safer Internet Checklist Response. Updated June 2021**)

Email

Staff and pupils (*where appropriate*) at this school use **Office365** for all school emails. 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 or Headteacher should be informed immediately. In addition:

- Staff or pupil personal data should never be sent, shared or stored on email.
- Internally, staff should use the school network, including when working from home when remote access is available via **Office 365**.
- 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 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.

School website

The school website is a key public-facing information portal for the school community (*both existing and prospective stakeholders*) with a key reputational value. The site is managed hosted by **Greenhouse Content Management System**.

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. 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.

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. Permission may be given for the following:

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

Whenever a photo or video is taken or made, the member of staff taking it will check the latest database (*held on the school system*) before using it for any purpose.

Any pupils shown in public facing materials are never identified and photo file names or 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 and personal equipment for taking pictures of pupils, and where these are stored. At St Paul's C of E VC Junior School, no member of staff will ever use their personal phone to capture photos or videos of pupils OR where given permission by the Headteacher, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

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

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (*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. Pupils are taught about how images can be manipulated in their online safety education 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.

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

Pupils are allowed to bring mobile phones in for emergency use only. At the start of the school day all mobile devices are handed to the class teacher who will then store the device in a locked safe. Pupils are not allowed access to their mobile devices during the school day. At the end of the school day children are not allowed to use their devices while on school property.

Any attempt to use a phone on the school site without permission or to take illicit photographs or videos will lead to 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.

All staff who work directly with children should leave their mobile phones (*and wearable technology*) on silent and only use them in private staff areas during allocated school hours (*break and lunchtimes*). Child or staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

Volunteers, contractors, governors should hand their phones in to reception where they will be secured in a locked safe. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (*for contractors to take photos of equipment or buildings*), permission of the headteacher should be sought and this should be done in the presence of a member staff.

Parents are asked to leave their phones in their pockets and turned off when they are on site. We operate a '*Meet your child with a smile, not a mobile*' policy at St Paul's C of E VC Junior School. Parents should ask permission before taking any photos (leaver's services, church services) and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network and internet access on school devices

Pupils are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use within the framework of the acceptable use policy. All such use is monitored.

Home devices are issued to some students under the *DfE technology support scheme*. These are restricted to the apps and software installed by the school and monitored using **MOSYLE**. They may only be used for learning and reasonable and appropriate personal use at home (*Internet research linked to subject*), but all usage may be tracked. The devices are filtered.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during allocated school hours.

Volunteers, contractors, governors have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.

Parents have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.

Trips and events away from school

For school trips and events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils 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.

Teachers will only use the school monitored and controlled social media accounts.

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.

Schedule for Development, Monitoring and Review

The Implementation of the online safety policy will be monitored by a working group (*online safety lead, child protection lead, link governor*) meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by the online safety working group by looking at:

- Log of reported incidents
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

The online safety policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to online safety or incidents that have taken place.