

St Paul's C of E Primary School

Life in all its fullness

St Paul's C of E VA Primary School

Contents

Background to this policy	2
Rationale	3
Other web technologies.....	5
The Online Safety Curriculum.....	7
Continued Professional Development	8
Parental involvement	8
Monitoring, and Averting Online Safety Incidents.....	9
Responding to Online Safety Incidents	10
Future Improvements	10
Equal Opportunities	11
Mobile Phones and Use of Mobile Data in School	11
Safeguarding Diagram Procedure	17
External to this document:	
EYFS, KS1 and parent Acceptable Use Agreement	Appendix 1
KS2 and parent Acceptable Use Agreement.....	Appendix 2
Staff, Governor and Volunteer Acceptable Use Agreement.....	Appendix 3
Digital Safety Posters	Appendix 4

St Paul's C of E VA Primary School Digital Safety Policy

Background to this policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

Online safety in schools is primarily a safeguarding concern and not a technology one. Therefore, this policy should be viewed alongside other safeguarding policies and approaches including, but not limited to:

- Safeguarding and Child Protection policy
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection policy
- Freedom of information policy
- GDPR Policy data retention policy
- Anti-Bullying Policy
- School Complaints Procedure
- Whistle Blowing Policy
- National Centre of Computing Excellence Progression in Computing Materials
- Privacy notices

This policy must be read alongside the staff, volunteer and pupil Acceptable Use Policies (AUPs).

These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- The Headteacher: Helen Darrell
- The Designated Safeguarding Leads: Helen Darrell, Natasha Thake and Sarah Day
- The Computing Subject Leader: Sarah Abrey (maternity – covered by NT)
- Cambridgeshire Local Authority Advice from model policies: Cambridgeshire Education ICT Service
- The governor responsible for Safeguarding: Imogen Nay

It was presented to the governing body on and ratified in July 2026 and will be formally reviewed in **June 2027**.

St Paul's C of E VA Primary School Digital Safety Policy

- This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via our internal communications, in a staff meeting, is readily available on the school google drive, and has also been made available to parents on the website.
- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As online safety is an important part of our school's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale

Digital technology and its use has now become a central part of pupils' everyday lives. We aim for pupils to be both confident and competent in their use of a wide range of digital technology and to provide competence, challenge and opportunities for pupils to extend their capability. We aim to empower pupils and adults with skills to access lifelong learning and employment. Digital technology covers a wide range of resources, including web-based and mobile learning that can take place using computers, laptops, chromebooks, digital cameras, voice recorders, Micro: bits and tablets.

All computers, laptops, chromebooks, computer screens and tablets in school have access to internet technologies. It is therefore necessary to provide guidance to reflect the school's rules about appropriate and acceptable use of it. Digital technology using the internet is a valuable resource that can raise educational standards by offering both pupils and teachers opportunities to access websites, learning platforms, virtual learning environments, email and instant messaging (IM), blogs, podcasting, video broadcasting, music downloading, gaming and many more. However, some of the information found on these internet technologies may be inappropriate for pupils. The Headteacher, Safeguarding lead, Computing Leader and governors have a duty to ensure that all adults and pupils in our school are aware of the procedure for dealing with this problem should it arise.

This policy and the agreements within (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile digital technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc.); and technologies owned by staff, governors, visitors and pupils, but brought onto school premises (such as laptops, mobile phones, cameras, tablet devices, portable media players, etc.). This policy will help to define appropriate and acceptable use by all staff, governors, visitors and pupils (**Appendix 1, 2 and 3**) and offer a focus for constant review.

The risks pupils may face can broadly be categorised into the 4 C's: **Contact, Content, Conduct, and Commerce** (*Keeping Children Safe in Education, updated annually*) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information

St Paul's C of E VA Primary School Digital Safety Policy

- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- Phishing or financial scams
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops / desktops - staff devices can also be used at home in accordance with the **staff AUP (Appendix 3)**, particularly with regard to GDPR.
- Staff have access to school systems beyond the school building (e.g. Management Information Systems – office and finance use, Microsoft 365 - email and office systems and Google Workspace – teaching storage and online teaching platforms).
- Class iPads and Interactive Whiteboards
- Staff level internet access
- Social media platforms: School Instagram account (access through Headteacher's iPad only)
- Online tools providing learning support materials

Pupils:

- Curriculum laptops / iPads / Chromebooks including filtered access to the Internet and pupil level access to areas of the school network used in accordance with the **EYFS and KS1 AUP or KS2 AUP (Appendix 1 and 2)**
- iPads and peripherals including programming resources: Micro: Bits, Data loggers, Beebots
- Cloud platforms (Google Workspace) and online tools providing pupils with access within and beyond the school gates: TTRA/Numbots, French – Planet Languages

Where the school changes the use of existing technology or introduces new technologies which may pose risks to users' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

St Paul's C of E VA Primary School Digital Safety Policy

Other web technologies

We use a range of web-based resources to communicate, record and support your children's learning. Here are the names of some of them and what we use them for:

Twinkl	This provides staff with resources to support planning, teaching and displays.
SchoolGrid	This is the school's lunch ordering system that provides parents the opportunity to order their children's lunches online. Staff are able to check to ensure all lunches are ordered.
Kapow	This is the planning sequence used to support teacher's delivering the music and design and technology curriculum.
Literacy Tree	This website supports the delivery of English providing planning support for the chosen texts supporting topic teaching.
Bromcom	This is used for the teachers to register the children twice a day and logs all the children's information digitally.
Letterjoin	This website supports the teaching of handwriting with posters, resources and planning sequence.
Tapestry	In Reception, we use educational software called 'Tapestry' to enable every child in the class to have their own individual learning journal. Parents log on with a secure username and password and are able to access their child's journal. Parents are only able to view their own child's journal and all information is stored on a highly secure server, which is monitored closely. They sign a form to say they will not post pictures to social media.
White Rose	This is a website to which we have a premium subscription to support teachers delivery of maths and science learning across the school.
Phonics Play	This subscription website is used by KS1 staff to support planning and delivery of phonics teaching and interventions.
Gsuite	Gsuite is a full range of online tools the children can use to create learning both in school and at home.
School Website	used to share information about our school with the wider community
Microsoft365	staff and class emails and online storage for office staff

St Paul's C of E VA Primary School Digital Safety Policy

Spotify	for music playlists - always checked by staff before use
Safeshare	a website used to share youtube videos without adverts through the videos or surrounding them
NFER	data tracking for termly reading, spelling, grammar and punctuation assessments for all classes
Primary Languages Network	French language scheme and online access for children at home
TTRA/ Numbots	children use this for weekly maths homework
National Governance Association	use by governors for information and training
Literacy Shed and Spelling Shed	used for spelling teaching and home learning
Scratch	used for coding in lessons and Code Club
National Centre of Computing Excellence	computing scheme for teaching Years 1-6
Paintz.app	web-based art website used to support computing lessons
Computing at school	online support, training and resources for Computing
National Centre for Excellence in Teaching of Mathematics	supporting activities for challenges and support in maths teaching and learning
Cbeebies	We may use alphablocks/numberblocks/factual programmes to support curriculum activities
TES Edukey (My Concern)	our secure logging of safeguarding or pupil behaviours
Primary PE Planning	Our PE planning and progression documents along with supporting video
Schools Swimming	Swimming teaching supporting documents
Access art	art scheme along with additional teaching and learning documents

St Paul's C of E VA Primary School Digital Safety Policy

The Online Safety Curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the [National Curriculum for Computing \(England\)](#) and the statutory [Relationship and Health Education](#).

At **St Paul's** we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

Our online safety curriculum is based on the National Centre of Computing Excellence Computing Scheme (built into Computing teaching), and the Cambridgeshire PSHE Service Primary Personal Development Programme, with reference to UKCIS's Education for a Connected World

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as researching, blogging and communicating in appropriate online environments.
- Focus events to raise the profile of online safety for our pupils and school community
- A flexible curriculum which is able to respond to new challenges as they arise.

Our overall aim is to ensure pupils are responsible, competent, confident and creative users of information and communication technology.

- KS1 will use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact when using digital devices.
- KS2 will use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

To support the delivery of our Computing curriculum we are following the National Centre for Computing Excellence scheme for Year 1-6. This covers all four aspects of Computing and Coding every year.

All pupils will be reminded of the importance of safe use of digital technologies and have year group specific reminders of these rules. In Reception they use the 'digi-duck poster', year 1 'bee safe', year 2 'smartie the penguin', year 3 and 4 have 'be smart online', year 5 and 6 use 'stay smart'. The children were involved in picking a suitable poster for the year groups.

St Paul's C of E VA Primary School Digital Safety Policy

Continued Professional Development

Staff at **St Paul's** receive up-to-date information and training on online safety in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

Nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

New staff, governors and volunteers receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online (<https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/professional-reputation>).

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Parental involvement

It is our firm belief that parents/carers should be involved in promoting digital safety in and outside school. Sharing open and honest discussions with children about digital technologies enables them to be open and honest about their use of digital technologies and to feel safe if they find content that makes them feel uncomfortable, bothers or upsets them. Children who feel secure in doing this are more likely to be resilient online, self-regulate how they use digital technologies and will be more self-empowered.

We want to encourage and support parents/carers in supporting their children when using digital technologies. We wish to reassure parents/carers that they do not need to know all about technology to keep their child safe online, by having open and honest communications about what digital device they are going to use (computer, tablet, x-box etc.), if they are interacting with others and if so who the other people are (are they talking to their friends from school or people they have not met?) and what they are going to do on the device (use the internet, game, watch YouTube etc.).

Parents/carers are required to make a decision as to whether they consent to images of their child being used in the public domain (on school website, displays around the school, in the prospectus, on tapestry etc.)

Parent/carers will be provided with relevant Digital Safety information where appropriate in the form of:

- Information and celebration events
- Posters
- Digital Safety area on the School website
- Newsletter 'Top Tips'

St Paul's C of E VA Primary School Digital Safety Policy

Monitoring, and Averting Online Safety Incidents

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include:

- Secure, private EastNet internet connection with a direct link to the National Education Network. This is provided and maintained The ICT Service on behalf of the local authority.
- Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites.
- Enhanced web filtering provided to all EastNet sites as standard.
- Antivirus package provided as part of EastNet Connection.

Adult and pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- For pupils, appropriate levels of supervision when using online technologies.
- For all school devices staff, volunteer, governor or pupil use, auto-generated alerts which flag up activity in specific safeguarding categories which may raise child protection concerns.
- For all school devices staff, volunteer, governor or pupil use, use of additional reporting tools to monitor and investigate use of the device.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network, cloud services and MIS systems.
- Supply teachers can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network.

Whilst we recognise that it is impossible to eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

St Paul's C of E VA Primary School Digital Safety Policy

Responding to Online Safety Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, **St Paul's** will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts, restricted access to systems as per the school's AUPs or reporting incidents to the police and other authorities– see appendix).

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the Headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if they deem it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Future developments

We are constantly reviewing the digital devices and technology we use in school to provide the pupils with the best computing experiences.

We are working on ensuring children are developing their knowledge and skills throughout their journey through St Paul's. We are continuing to develop our Computing curriculum and enhancing activities as well as sharing with the children potential uses for the skills they gain in computing.

We have set up and are continuing to explore the wide range of resources offered by 'Google for Education' with the children which offers a Google hosted secure school network for email, calendar, chat, document storage and creating/editing of a wide range of documents. This is a safe and secure environment in which pupils can learn to communicate appropriately using email, safely chat with friends and create and edit work. The benefit of Google for Education is it cannot be accessed by anyone not in

St Paul's C of E VA Primary School Digital Safety Policy

the school network, is constantly monitored by the school and allows pupils to use it both in school but also at home. Staff have explored possibilities to develop their teaching using this over the past couple of years. It has been well used while home learning was needed and will be continually explored in school to enhance learning.

Technologies such as a class set of BBC Micro: Bits to allow the delivery of a more in-depth study of Computing these have arrived and projects are being built-in to KS2. The school set of ipads should be looked at closely for replacement as they are becoming less useful due to the inability to add new apps because of their age - however this does not impact the fundamental computing curriculum delivery currently. The batteries on the laptops have recently been replaced giving them a longer life-span allowing devices to be used for Computing lessons and then Code Club as well now the batteries have gone from 30-minute life span to 10 hours.

Equal opportunities

All pupils are given an equal opportunity regardless of gender, ethnicity, ability or age, to work independently, collaboratively or with support from adults (teachers, support staff and parents/carers) using digital technology. Care and consideration for people and equipment is actively encouraged at all times.

Teachers will strive to ensure that a pupil who does not have access to internet technologies at home has an equal chance to access internet technologies in school, so that they do not miss opportunities to enhance and support any work being undertaken.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of digital safety. Internet activities are planned and well managed for these pupils.

Mobile Phones and Use of Mobile Data in School

Keeping Children Safe in Education (September 2022) acknowledges that "many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G)." It highlights the need for schools to have a clear policy statement on, and carefully consider "*how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*".

1.0 Introduction and aims

It is widely recognised that many children have access to personal communication devices including mobile phones, smart phones and smart watches. Children using these devices are likely to have unlimited and unrestricted access to the internet via mobile networks such as 3G, 4G, 5G, Airdropping and 'Nearby Share' (see Annex 1 for more details). For many these devices can provide security and reassurance; however there also associated risks. Safeguarding of children within the school is paramount.

St Paul's C of E VA Primary School Digital Safety Policy

Effective guidance is in place to avoid the use of mobile, smart phone and smart watches causing unnecessary disruptions and distractions within the workplace, and to ensure effective safeguarding practice is promoted to protect against potential misuse.

The terms 'phone' or 'mobile phone' in this guidance denotes personal mobile phones, smart phones, airpods, iPods, iPads, MP3 players, MP4 players and smart watches.

1.1 The guidance aims to:

- Set out clear guidance for the use of mobile phones for staff (including supply staff), governors, pupils and volunteers
- Set out clear guidance for visitors and contractors.
- Ensure robust safeguarding
- Support schools' other policies relating to child protection and behaviour

2.0 Staff responsibilities

All staff (including teachers, support staff, and supply staff) may wish to have their personal mobile phones at work for use in case of emergencies, however, there is a clear expectation that all personal use is limited to areas and times when there are no children present or likely to be present.

2.1 All staff:

- The school expects staff to lead by example and therefore should not make or receive personal calls, or texts (via mobile phone or smart watch), whilst children are present or during contact time (8:45am-12pm and 1-3.30pm).
- Staff (including volunteers and supply staff) should only use their mobile phones and smart devices for personal contact in designated areas: staff room, office or off-site.
- Other than in agreed exceptional circumstances, mobile phones should be switched off or on silent and left in a safe place (lockers are provided for TAs in the staffroom and teachers have classroom cupboards) and smart watches silenced during lesson times.
- The school retains no liability for any device that is brought into school which is either lost, stolen or damaged.
- The school retains no liability for any device that is used in a manner that is against the owner's consent.

2.2 Safeguarding

- Staff should not contact pupils or parents from their personal mobile phone in or out of school time or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, a school telephone should be used.
- Staff should not share personal contact details through social media and messaging apps.

St Paul's C of E VA Primary School Digital Safety Policy

- Staff should regularly monitor and update their privacy settings on social media sites.
- Staff should never accept a 'friend request' or respond to any posts that may deliberately or inadvertently include them but inform their line manager or Senior Leader of the contact.
- Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.
- Staff are not permitted to use their devices to take photos or videos of pupils or anything else (e.g., work) that might identify the pupil.
- If photos or videos are being taken as part of the school curriculum or for promotional purposes, then school equipment must be used.
- Staff should not allow themselves to be photographed by a pupil(s) on their personal devices.

2.3 Using a personal mobile for work purposes

In some circumstances, it may be appropriate for staff to use a personal mobile phone for work purposes. Where possible this should always be agreed with a line manager or Senior Leader in advance. Such circumstances may include, but are not limited to:

- Emergency evacuations
- Parental contact in emergency's (mobile phones setting that allow for the number not to be identified should be used)
- Weather or Public Health (outbreaks/pandemics) longer term closures of schools

This guidance should be seen as a safeguard for members of staff and the school. Any breach of school policy may result in disciplinary action against that member of staff.

2.4 Personal mobile for trips and residential visits

On school trips and residential visits, all adults accompanying the school trip or residential visit will be allowed to carry their mobile phones with them. However, these must all be kept out of sight of the children throughout the trip unless under the following circumstances:

- If the use of a phone is needed to update school on arrival times/delays etc. then only the trip leader will be permitted to use theirs.
- In case of an emergency where the groups are split up and another adult urgently needs to report a missing child or call emergency services they will be able to use their phone
- If the school office is closed there will be a nominated person to take any emergency calls

Only the trip leader is permitted to use their phone unless the above extreme emergency circumstances occur.

St Paul's C of E VA Primary School Digital Safety Policy

Staff will not give their personal phone number to any volunteers. In case of the extreme emergency, when the group is not together, described above, volunteers will call the school office who will then contact the trip leader.

3.0 Pupils:

We recognise that the some pupils will bring mobile phones to school, and some may wear a digital watch with additional capabilities. Expectations around phone and smart watch usage should be clearly communicated to all pupils and parents.

- Pupils are not permitted to bring mobile phones to school unless in Year 6, where they may walk home alone.
- If it is deemed necessary for a Year 6 pupil to bring a mobile phone to school, (e.g., because they travel to and from school independently), then the expectation is that the pupil **turns off** and hands their phone into the class teacher on arrival and it will be returned to them at the end of the school day.
- The school retains no liability for any device that is brought into school which is either lost, stolen or damaged.
- The school retains no liability for any device that is used in a manner that is against the owner's consent.

4.0 Parents, visitors and contractors:

During the school day, parents, visitors and contractors are respectfully requested not to use their mobile phones at all on the school site/in any area where children/young people are present.

- Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by children to avoid any unnecessary disturbance or disruption to others.
- Should phone calls/and or texts need to be taken or made, visitors and parents are asked to leave the premises to do so or go to the school office.
- Should photos, phone calls/and or texts need to be taken or made in location where they are working, contractors are to be supervised by a member of staff. Photos should not contain children or any material that identifies children, it should also not record GPS data location tracking.
- Photos of children must not be taken without prior discussion with a member of the Senior Management Team and in accordance with the UK *General Data Protection Regulations (GDPR)* and the *Data Protection Act 2018* and using the 'Use of images consent form' (please see within policy under: Guidance for schools and other establishments on the use of images). Any individual bringing a personal device into the school must ensure that it contains no inappropriate or illegal content.

St Paul's C of E VA Primary School Digital Safety Policy

- The school retains no liability for any device that is brought into school which is either lost, stolen or damaged.
- The school retains no liability for any device that is used in a manner that is against the owner's consent.

5.0 Inappropriate or illegal content:

Where there is a suspicion that the material on a mobile phone may be unsuitable and may constitute evidence relating to a criminal offence, the allegations process will be followed (please refer to the school's 'Safeguarding and Child Protection Policy').

6.0 Governor whatsapp group/messaging:

- Governor Code of Conduct will include reference to WhatsApp use guidelines

Related Policies and guidance:

Safeguarding and Child Protection Policy (updated annually in September)

Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings February 2022

Keeping Children Safe in Education (updated annually)

Guidance for schools and other establishments on the use of images (September 2023)

Data Protection: A toolkit for schools, DfE, (August 2018)

Annex 1 - Airdrop and Nearby Share

Airdrop.

- AirDrop is a feature available on iPhones and Mac computers (iOS 7, iPadOS 13, OS X 10.10, or later required).
- It lets physically close Mac and iOS devices share files, photos, websites etc.
- There are no size limits on files.
- It uses Bluetooth and Wi-Fi to transmit the files.
- AirDrop automatically detects nearby supported devices within a maximum distance of 30 feet.
- When a receiver of content is selected, they will be notified and offered the option to accept or decline the incoming file.

Nearby Share.

- Nearby Share is available on Android 6.0+ phones.

St Paul's C of E VA Primary School Digital Safety Policy

- Like AirDrop, it allows users to instantly share files, links and pictures with people around them.
- It also works through Bluetooth or WiFi.
- When Nearby Share is turned on, a list of devices available within sharing proximity is visible.
- When a receiver of content is selected, they will be notified and offered the option to accept or decline the incoming file.

Safeguarding risks posed by both Airdrop and Nearby Share.

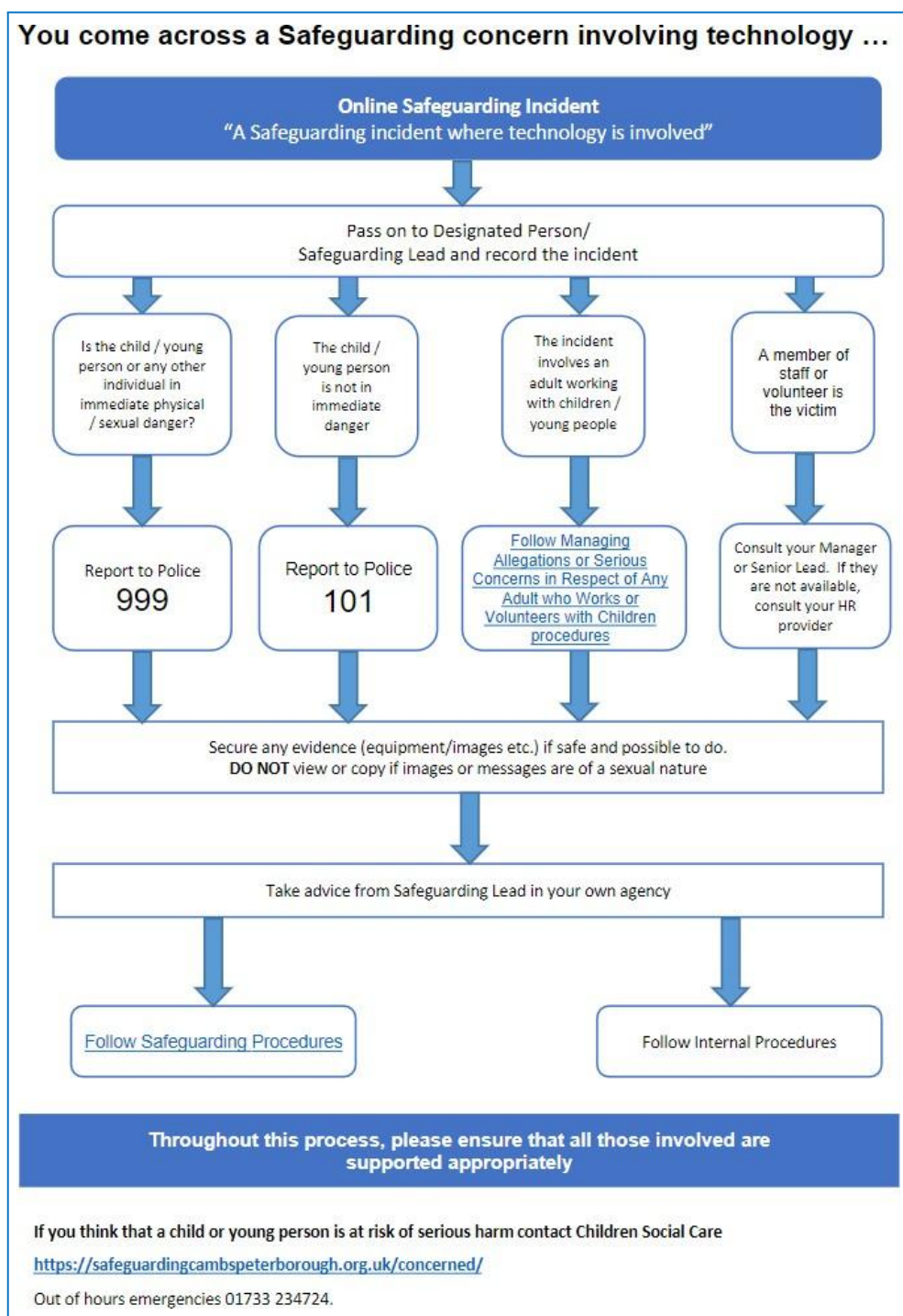
- Being exposed to age-inappropriate sexualised and/or violent content.
- Photo sharing as a form of cyberbullying, with the person featured in the image being the target.
- The sharing of self-generated sexual imagery, with or without the permission of the original image/video creator.
- Images of teachers or other staff members shared as part of teacher targeted bullying, including 'upskirting' images (the practice of taking an illegal photo of someone's genitals or genital area, without consent).

If a member of staff or a pupil report receiving inappropriate content then the school must follow their Safeguarding and Child Protection Policy and procedures.

St Paul's C of E VA Primary School Digital Safety Policy

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated below.

Figure 1. Responding to a Safeguarding Incident where Technology is Involved



St Paul's C of E VA Primary School Digital Safety Policy

New Children Board Procedures | Cambridgeshire and Peterborough Safeguarding Partnership Board
(safeguardingcambspeterborough.org.uk)