All Saints CE Primary School Online Safety and Acceptable Use Policy

Designated Safeguarding Lead (s):

Mrs Jane Hall, Headteacher
Mrs J. Ellison, Assistant Head
Mrs C. Darling-Chalke, Inclusion Leader

Computing Lead Teacher: Mr Dan Boorman

Named Governor with lead responsibility/Safeguarding Governor: Ms Becca Higham

This policy will be reviewed annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

1. Policy Aims

All Saints Church of England Primary School is committed to providing a safe and secure environment where pupils flourish. Under our Christian values of Love, Hope and Community, we recognise that Safeguarding, including online safety, and promoting the welfare of children is everyone's responsibility.

- This Online Safety Policy has been written by All Saints C of E Primary School, involving staff, pupils and parents/carers, building on the County Council online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education", Early Years and Foundation Stage and the Safeguarding Children Partnership procedures , DfE Filtering and Monitoring Standards 2023

- The purpose of All Saints C of E Primary School online safety policy is to:
    - Safeguard and protect all members of All Saints C of E Primary School community online
    - Identify approaches to educate and raise awareness of online safety throughout the community
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns

- All Saints C of E Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

2. Policy Scope

- All Saints C of E Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online
- All Saints C of E Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life
- All Saints C of E Primary School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
  - Anti-bullying policy
  - Acceptable Use Policies (AUP) - including children's Technology Charter
  - Behaviour policy
  - Child protection policy
  - Safeguarding policy
  - Confidentiality policy
  - Curriculum policies such as: Relationships and Sex Education (RSE)
  - Data security
  - Image use policy
  - Mobile Phone policy
  - The School's Safeguarding Curriculum

3. Monitoring and Review

All Saints C of E Primary School will review this policy at least annually.

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure we have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate and will work with the Governor for safeguarding to report to the governing body on online safety incidents, including outcomes.

Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The school has appointed Jane Hall, as Designated Safeguarding Lead to be the online safety lead with the assistance of the Computing Leader Mr Dan Boorman
- All Saints C of E Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including an AUP, which covers acceptable use of technology (Children and staff)
- Ensure that suitable and appropriate filtering and monitoring systems are in place (operated by our IT Provider, Harrap)
- Work with technical staff to monitor the safety and security of school systems and networks

- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety
- Support the Designated Safeguarding Lead by ensuring they has sufficient time and resources to fulfil their online safety responsibilities
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement

4.2 The Designated Safeguarding Leads (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches. School website updated regularly
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- Report online safety concerns, as appropriate, to the SLT and Governing Body
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input
- Meet regularly, at least once per term, with the governor with a lead responsibility for safeguarding and online safety

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies
- Read and adhere to the online safety policy and technology AUP (these must be signed by staff)
- Take responsibility for the security of school systems and the data they use, or have access to
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- Embed online safety education in curriculum delivery, wherever possible (see non-negotiables on teaching of computing which includes online safety)
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care

- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures including recording incidents
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally
- Take personal responsibility for professional development in this area

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age-appropriate online safety education opportunities
- Contribute to the development of online safety policies
- Read and adhere to the school AUPs (All Saints Technology Charter – displayed in all classrooms)
- Respect the feelings and rights of others both on and offline
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues

4.6 It is the responsibility of parents and carers to:

- Read the school AUP/class Charter (on our school website and sent home) and encourage their children to adhere to them
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home
- Role model safe and appropriate use of technology and social media
- Abide by the school's home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online

- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Contribute to the development of the school online safety policies
- Use school systems, such as learning platforms (Google classroom), and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - ensuring education regarding safe and responsible use precedes internet access.
    - including online safety in the PSHE, RSE and Computing programmes of study, covering use both at home school and home.

We use the Teach Computing Scheme of Work. The units include specific teaching on how to keep safe online. We periodically have visitors and guest speakers into school to work with children on online safety. RSE Scarf units for each group also reinforce our online safety curriculum.

We ensure that we:

- reinforce online safety messages whenever technology or the internet is in use
- educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- teach pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

- The school will support pupils to read and understand the AUP (School Technology Charter) in a way which suits their age and ability by:
    - involving the Cyber Ambassadors in writing the Charter
    - seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation
    - displaying Acceptable Use posters in all rooms with internet access
    - informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation
    - rewarding positive use of technology by pupils
    - implementing appropriate peer education approaches
    - providing online safety education and training as part of the transition programme across the key stages and when moving between establishments
    - using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches

5.1.1 Vulnerable Pupils

All Saints C of E Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
All Saints C of E Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
All Saints C of E Primary School will seek input from specialist staff as appropriate, including the SENDCo and Inclusion Lead and ELSA/Wellbeing Lead as well as outside agencies.

5.2 Training and engagement with staff

The school will:

- provide and discuss the Online Safety Policy with all members of staff as part of induction
- provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates as part of ongoing safeguarding training. This will cover the potential risks posed to pupils (Content, Contact, Conduct and Commerce) as well as our professional practice expectations/ Code of Conduct
- make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices
- make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school
- highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community

5.3 Awareness and engagement with parents and carers

All Saints C of E Primary School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The school will build a partnership approach to online safety with parents and carers by:

- providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes/fayres and sports days
- drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus/brochure and on our website
- requesting that they read online safety information as part of joining our school, for example, within our home school agreement

- requiring them to read the school technology AUP (School Technology Charter) and discuss its implications with their children

6. Reducing Online Risks

All Saints C of E Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material

All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

All Saints C of E Primary School uses a wide range of technology. This includes access to:

- computers, laptops, Chrome books and other digital devices
- internet which may include search engines and educational websites
- digital cameras

All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. Our children are taught to search safely and appropriately using search engines.

The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.

Supervision of pupils will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1

- Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability

Key Stage 2

- Pupils will use age-appropriate search engines and online tools
- Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability

7.2 Managing Internet Access

The school will maintain a written record of users who are granted access to the school's devices and systems.

All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

7.3.1 Decision Making

All Saints C of E Primary School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

The Designated Safeguarding Lead takes the lead responsibility for understanding the filtering and monitoring systems and processes in place. We follow Keeping Children Safe in Education and the Government's 'Meeting digital and technology standards in schools and colleges' guidance.

The School uses:

- Harrap – Firebox M290 on-premises for filtering and firewalling
- WatchGuard Basic security protection against intrusion, viruses, known ransomware at the firewall
- SENSO cloud online filtering system
- URL filtering to block unknown malicious sites and sites that staff and/or pupils should not have access to which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature
    - The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school works with Harrap IT to ensure that our filtering policy is continually reviewed
- Filtering also includes protection in foreign languages which may be used by our children

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, they will be required to report it to a member of staff immediately

- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff
- The breach will be recorded and escalated as appropriate
- Parents/carers will be informed of filtering breaches involving their child

Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by the:
  - *supervision of all children using the internet by an appropriate adult.*

The school has a clear procedure for responding to concerns about identified via monitoring approaches.

- *staff will report any issues to the DSL regarding child/children which will be recorded on CPOMS*
- *parents will then be informed as appropriate*

All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.3 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998.

- Full information can be found in the school's Data Protection policy and the arrangements for GDPR.

7.5 Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

- virus protection being updated regularly.
- encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- not downloading unapproved software to work devices or opening unfamiliar email attachments.
- regularly checking files held on the school's network,
- the appropriate use of user logins and passwords to access the school network.
  - specific class logins and passwords will be enforced for all
- all users are expected to log off or lock their screens/devices if systems are unattended.

Further information about technical environment safety and security can be found in the technology AUP.

7.5.1 Password policy

All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.

From year R, all pupils are provided with their own class username and private passwords (via QR code) to access school systems; pupils are responsible for keeping their password private.

We require all adult users to:

- use strong passwords for access into our system
- change their passwords every time they are requested
- always keep their password private; users must not share it with others or leave it where others can find it.
- not to login as another user at any time unless using a class login
- Keep computers/laptops locked when not in use

7.6 Managing the Safety of the School Website

The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
The administrator account for the school website will be secured with an appropriately strong password.
The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online

The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image use policy, Data security, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones (Code of conduct). We also follow guidance re: sharing non- identifiable images on our website and school recommended actions.

7.8 Managing Email

Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of Conduct.

- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the school community will immediately tell (DSL – Jane Hall, Head teacher) if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.

The school uses CPOMs to record any safeguarding concerns linked to Technology use.

7.8.1 Staff

The use of personal email addresses by staff for any official school business is not permitted.
All members of staff are provided with a specific school email address, to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

7.8.2 Pupils

Pupils will use school provided class email addresses for educational purposes. This is as part of the children's QR code log-in. Children do not use email addresses to send messages.

7.10 Management of Learning Platforms

- All Saints C of E Primary School uses its own network provided by Harrap and Googles classroom its official learning platform
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities
- Only current members of staff, pupils and parents will have access to the LPs
- When staff and/or pupils' leave the school, their account log on or rights to specific school areas will be disabled or transferred to their new establishment
- Pupils and staff will be advised about acceptable conduct and use when using the LP
- All users will be mindful of copyright and will only upload appropriate content onto the LP

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- the user will be asked to remove any material deemed to be inappropriate or offensive
- if the user does not comply, the material will be removed by the site administrator
- access to the LP for the user may be suspended
- the user will need to discuss the issues with a member of leadership before reinstatement. e) A pupil's parent/carer may be informed
- if the content is considered to be illegal, then the school will respond in line with existing child protection procedures

Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Children's Progress

- The school uses Arbor to track pupils' progress and share appropriate information, especially attendance records with parents and carers. The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation.

In order to safeguard pupils' data:

- only school issued devices will be used for apps that record and store children's personal details, attainment or photographs
- **personal staff mobile phones or devices will not be used to access or upload content** to any apps which record and store children's personal details, attainment or images
- **school devices will be appropriately encrypted if taken off site**, to reduce the risk of a data security breach, in the event of loss or theft
- **all users will be advised regarding safety measures, such as using strong passwords and logging out of systems when not in use or on leaving a device unsupervised**
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images

8. Social Media

8.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members of All Saints C of E Primary School community.
The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of All Saints C of E Primary School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
All members of All Saints C of E Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
The use of social media during school hours for personal use is permitted but only on personal devices and within the staffroom during school breaktime hours.
Inappropriate or excessive use of social media during school/work hours or whilst using school devices, may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of All Saints C of E Primary School community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour Management and Child Protection policies.

8.2 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

Reputation
All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as strictly as they can
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the school

Members of staff are encouraged not to identify themselves as employees of All Saints C of E Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework.
Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles

Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.

If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.

Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.

Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Pupils will be advised:

- *to consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include*

real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs

- *to only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.*
- *not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.*
- *to use safe passwords*
- *to use social media sites which are appropriate for their age and abilities.*
- *how to block and report unwanted communications and report concerns both within school and externally*

9. Use of Personal Devices and Mobile Phones

See Mobile Phone Policy for details

9.1 Expectations

All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour Management, Child Protection and Safeguarding, Mobile Phone Policy, Social Media Policy

Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. Personal devices are not permitted to be used in any classroom.
All members of All Saints C of E Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
All members of All Saints C of E Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

As Per DFE Guiadnce, we are a mobile phone free site by default. Mobile phones and personal devices are not permitted to be used in specific areas within the school site, such as classrooms/music room/library/hall/playgrounds, the field, corridors, and toilets (during school and before and after school club hours). See Mobile Phone Policy for details.

The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.

All members of All Saints C of E Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour Management or Safeguarding and Child Protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child Protection, Safeguarding, Data Security and Acceptable Use.

Staff will be advised to:

- keep mobile phones and personal devices in a safe and secure place during lesson time
- keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times
- ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times
- not use personal devices during teaching periods, unless permission has been given by the headteacher, such as in emergency circumstances
- ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations- staff do not contact their own mobile phones to the school network

Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.

Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead – Jane Hall - Headteacher.

Staff will not use personal devices, such as: mobile phones, tablets or cameras:

- to take photos or videos of pupils and will only use work-provided equipment for this purpose
- directly with pupils, and will only use work-provided equipment during lessons/educational activities

If a member of staff breaches the school policy, action will be taken in line with the school behaviour, disciplinary and allegations policy.
If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Pupils' Use of Personal Devices and Mobile Phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
All Saints C of E Primary School expects pupil's personal devices and mobile phones to be handed into their classteacher during school hours. These will be labelled with the child's name and kept in a hidden secure place until the child collects it for going home.
If a pupil needs to contact his/her parents or carers they will be allowed to use the office phone. Parents are advised to contact their child via the school office during school hours.

Mobile phones or personal devices will not be used by pupils during lessons or formal school time. If a pupil breaches the school policy, the phone or device will be confiscated and will be held in the school office until it is collected by a parent or carer of the pupil.

School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour Management or Anti-bullying Policy, or could contain youth produced sexual imagery (sexting).

Searches of mobile phone or personal devices will only be carried out in accordance with the DfE's policy. (www.gov.uk/government/publications/searching-screening-and-confiscation)

Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies.
Mobile phones and devices that have been confiscated will be released to parents or carers through the school office
If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

All Saints actively seeks to restrict the use of mobile phones on its school site.

Parents, carers and visitors (including volunteers and contractors) must only use their mobile phones and personal devices in accordance with the school's Mobile Phone Policy and other associated policies, such as: Anti-bullying, Behaviour Management, Safeguarding, Child Protection and Image use.
The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of its expectations of use.
Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.
Content may be deleted or requested to be deleted, if it contravenes school policies.

9.5 Officially provided mobile phones and devices for school use.
Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
School mobile phones and devices will always be used in accordance with the Acceptable Use policy and other relevant policies (Safeguarding, Child Protection, Data Protection).

See Mobile Phone Policy

10. Responding to Online Safety Incidents and Concerns/Safeguarding Policy

All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
If the school is unsure how to proceed with an incident or concern, the DSLs will seek advice from the Education Safeguarding Team.
Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Police using 101, or 999 if there is immediate danger or risk of harm.
If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare
The DSLs will be informed of any online safety incidents involving safeguarding or child protection concerns.
The DSLs will record these issues in line with the school's child protection policy.
The DSLs will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Safeguarding Children Partnership thresholds and procedures.
The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse
Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations policy.
Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

All Saints C of E Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".

11.1.1 Dealing with 'Sexting'

If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:

- act in accordance with our Child protection and Safeguarding policies and the relevant Safeguarding Child Board's procedures
- immediately notify the Designated Safeguarding Lead
- store the device securely

If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image. It will carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
Inform parents and carers, if appropriate, about the incident and how it is being managed.
Make a referral to Specialist Children's Services and/or the Police, as appropriate.
Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.

The school will not:

- view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.2 Online Child Sexual Abuse and Exploitation

All Saints C of E Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
All Saints C of E Primary School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

If the school are made aware of incident involving online sexual abuse of a child, the school will:

- act in accordance with the school's Child protection and Safeguarding policies and the relevant Safeguarding Child Partnerships' procedures
- immediately notify the Designated Safeguarding Lead
- store any devices involved securely
- immediately inform police via 101 (or 999 if a child is at immediate risk)
- carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies)
- inform parents/carers about the incident and how it is being managed
- make a referral to Specialist Children's Services (if required/ appropriate).
- provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary

The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.

Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/

If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Police.

If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Education Safeguarding Team/Police by the Designated Safeguarding Lead.

If pupils at other schools are believed to have been targeted, the school will seek support from Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

All Saints C of E Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.

The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Police and/or the Education Safeguarding Team.

If made aware of IIOC, the school will:

- act in accordance with the school's child protection and safeguarding policy and the relevant Safeguarding Child Partnership procedures
- immediately notify the school Designated Safeguard Lead
- store any devices involved securely
- immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), police or the LADO

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:

- ensure that the Designated Safeguard Lead is informed
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- ensure that any copies that exist of the image, for example in emails, are deleted
- report concerns, as appropriate to parents and carers

If made aware that indecent images of children have been found on the school devices, the school will:

- ensure that the Designated Safeguard Lead is informed
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- ensure that any copies that exist of the image, for example in emails, are deleted
- inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate)
- only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- report concerns, as appropriate to parents and carers

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - ensure that the headteacher is informed
  - inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy
  - quarantine any devices until police advice has been sought

11.4 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at All Saints C of E Primary School.
Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy and the Safeguarding Policy

11.5 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at All Saints C of E Primary School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour Management, Safeguarding Policy.
All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
The Police will be contacted if a criminal offence is suspected.
If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Police.

11.6 Online Radicalisation and Extremism/PREVENT

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding/PREVENT/Child Protection Policy.

If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child Protection and Allegations policies/PREVENT/Channel referrals.

12. Artificial Intelligence (AI) and Online Safety

Our school recognises that artificial intelligence (AI) tools are increasingly part of the online world that children access. We ensure that pupils are taught, in an age-appropriate way, that AI can be helpful but may not always be accurate, safe or appropriate. Pupils are supported to understand that content created by AI should be checked carefully, and that they must not share personal information or use AI tools without adult guidance or permission. Staff carefully monitor and regulate the use of AI within school to ensure it is used safely, ethically and in line with safeguarding, data protection and curriculum expectations. Our approach promotes curiosity and learning, while prioritising children's safety, wellbeing and responsible digital behaviour. While AI can provide valuable opportunities for learning and creativity, it also presents specific online safety risks. These include the creation and sharing of misleading or harmful content, such as AI-generated images, videos, audio recordings and "deepfakes" that falsely appear to show real people saying or doing things they have not said or done. Pupils will be taught to think critically about online content, to question the authenticity of digital media, and to report any AI-generated content that causes concern. Staff will promote safe, responsible and age-appropriate use of AI technologies and will address any misuse, including the creation, sharing or use of AI-generated content that could harm, bully, embarrass, discriminate against or misrepresent others. The school will regularly review emerging technologies and provide guidance to pupils, staff and parents to help ensure AI is used safely, ethically and in accordance with the school's behaviour, safeguarding and online safety expectations.

12.1 Staff Use of AI tools

Staff must not input, upload, or otherwise share any pupil-identifiable or confidential information into artificial intelligence (AI) tools or platforms, including publicly available or personal AI applications, in order to protect data privacy and comply with data protection legislation.

The restriction on entering pupil data into AI tools is essential to protect children's personal information and uphold the school's legal responsibilities under data protection law. Any information that identifies a pupil is classed as personal data, and inputting this into AI systems constitutes data processing under UK GDPR. Many AI platforms, particularly open or free tools, may store, reuse, or use submitted data to train their models, meaning sensitive information could be retained, shared, or accessed beyond the school's control. This creates a risk of data breaches, unauthorised disclosure, or misuse of information, which could harm pupils and expose the school to legal and reputational consequences. Safeguarding pupil data is therefore a critical aspect of both privacy protection and wider safeguarding responsibilities within our school.

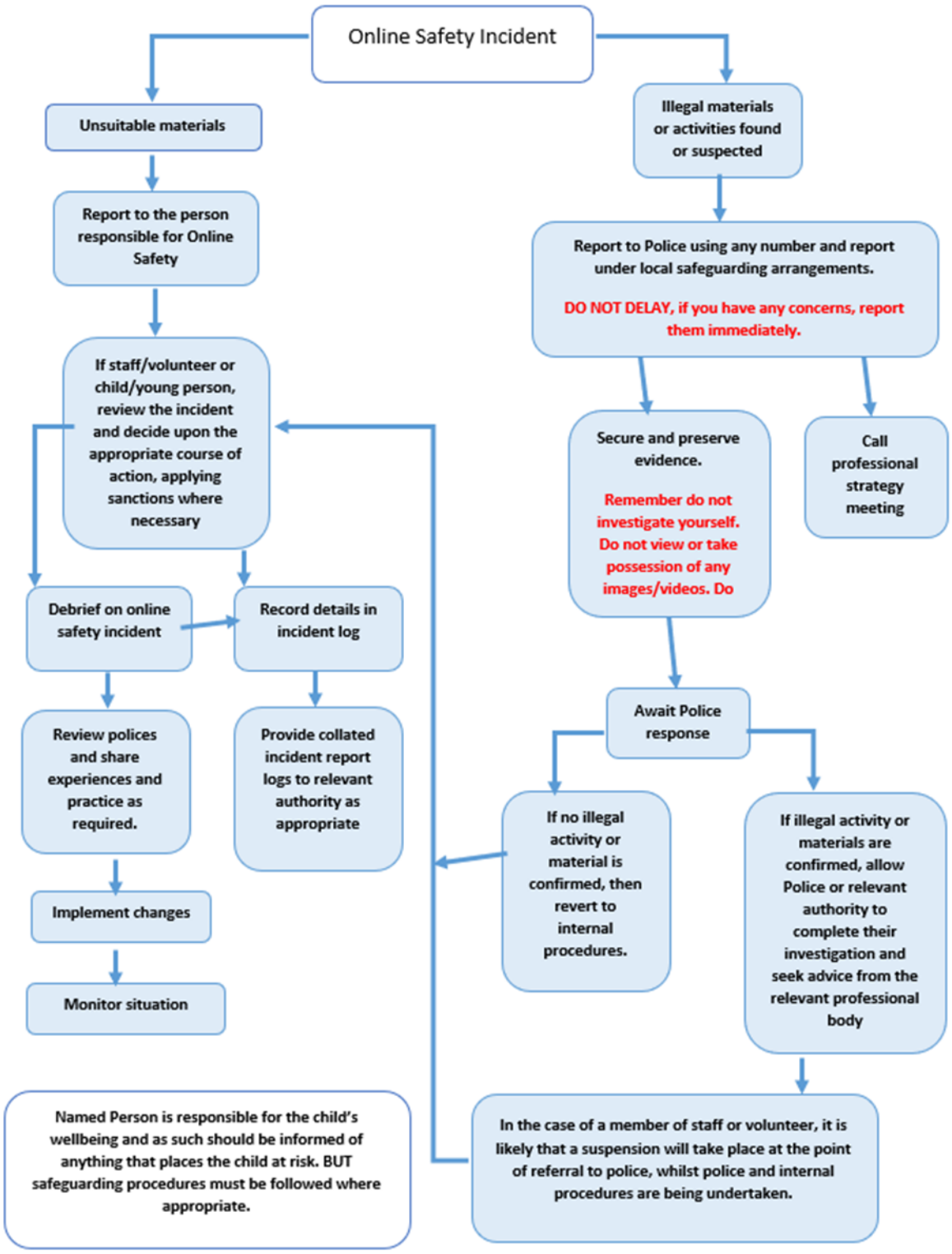
12.2 Robyn the Robot

We use Robyn which is an AI teaching assistant. Safety is of primary importance when using this AI tool and it is compliant with DfE AI Guidelines for school. Safeguards include:

- **Closed system:** Robyn's answers are based on what the teacher has taught in that lesson. It cannot access the wider internet, and if a pupil asks a question not related to the lesson, Robyn will decline to answer and will politely direct them back to the lesson topic
- **Content filtering:** All AI outputs are filtered for age-appropriate content before being spoken or displayed to pupils
- **No personal accounts:** Pupils don't log in or create accounts — there's no profile building or tracking of individual children
- **Teacher oversight:** Teachers can review all questions asked and answers given through the teacher port

This policy is reviewed at least annually by the Governing Body.

Policy agreed:	July 2026
To be reviewed:	November 2027


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

All Saints Church of England Primary School

Staff Code of Conduct and Acceptable Use for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Online and Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication
- I understand that I must not use the school ICT system to access inappropriate content
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own
- I will not install any software or hardware without permission
- I will follow the school's policy in respect of downloading and uploading of information and material
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use
- I will respect copyright, intellectual property and data protection rights
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher

- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children

The school exerciss its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

I have read, understood and agree to abide by the Policy for Online Safety and Staff Acceptable Use of ICT and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ……

DATE:……..….

NAME (PRINT): ……