All Saints' Church of England Primary School

Online safety Policy

Our theologically rooted vision:

'Seed fell on good soil. It came up, grew and produced a crop, some multiplying thirty, some sixty, some a hundred times.' (Mark 4.8)

Presented to and adopted by staff: November 2024

Presented to and adopted by governors: November 2024

Future Review Date: November 2025

Overview

All Saints' recognises that internet, mobile and digital technologies provide opportunities for children and young people to learn, socialise and play whilst understanding challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils and staff are supported to use the internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

Responsibilities

Safeguarding children, including online safety is everyone's responsibility; online safety is therefore not just the responsibility of the Computing coordinator/Designated Safeguard Lead/ Headteacher, it is a whole school approach.
The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.
All breaches of this policy that may have put a child at risk must be reported to the Designated Safeguarding Lead, [Rachael Parsons].

Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents:

- Safeguarding and child protection
- Keeping Children Safe in Education

- GDPR
- Health and safety
- Behaviour
- Anti-bullying
- PSHCE/RSE policies

Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Visiting online sites and downloading

Acceptable Use Policy (AUP)
This sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies. The AUP details how we provide support and guidance to parents / carers for the safe and responsible use of these technologies by adults and children. Each user signs a contract when they join the school to ensure that they know what is deemed 'acceptable use of the Internet'.

Internet Access
The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Internet access is planned to enrich and extend learning activities. When joining the school, parents of all pupils are asked to sign and return a consent form giving permission for their child to use the Internet.

- In Foundation Stage and Key Stage 1, access to the Internet is by adult demonstration and direct supervised access to specific, approved on-line materials.
- In Key Stage 2, pupils will work independently using the internet, but will not be left unsupervised. Pupils are given their own individual username and password to log onto the computer network on the laptops. When using the iPads, children use their individual username and password to access the internet via Smooth wall. Pupils are taught the importance of online safety and agree terms and conditions for acceptable Internet use. Pupils are taught to be critically aware of the materials they read and are made aware that information may be not always be reliable or accurate.

The school website:
- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

• Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Filtering and monitoring

• The School works in partnership with parents, Remedian and DFE to ensure that systems are in place to protect pupils.

- Children in Key Stage 2 are given their own individual username and password to log onto the computer network on the laptops. On the iPads, children use their individual username and password to access the internet via Smooth wall.

• If staff or children discover unsuitable sites, the URL (address) and content must be reported to Remedian via the Computing coordinator, the ICT log or the office staff. This is also monitored by Smoothwall who will alert school staff.

• Any material that the school believes to be illegal must be referred to the Internet Watch Foundation (IWF).

Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required.

Photographic, video and audio technology

• Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.

• Staff may use photographic or video devices to support school trips and curriculum activities. School equipment should be used for this purpose• Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.

• Pupils should always seek the permission of their teacher before making audio or video recordings within school grounds.

Mobile Phones (see Mobile Phone Policy)

• Children are not encouraged to bring mobile phones in school and are not allowed to use them in school. If a child needs to bring their mobile phone (in agreement with staff) they must be handed to a member of staff to be kept securely until the end of the day.

• Staff must have their mobile phones on 'silent' and out of sight during teaching times.

• The sending of abusive or inappropriate text messages is strictly forbidden.

Chat and instant messaging

• Pupils will not be allowed access to public or unregulated chat rooms.

• Pupils will not access social networking sites for example 'Whatsapp', 'Facebook', 'Twitter', 'Instagram 'etc.

• Any form of bullying or harassment is strictly forbidden.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Use the school's hardware and Wi-Fi facilities for running a private business
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the headteacher.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff (pupils) or the Headteacher/DSL/senior teacher on site (staff issues and staff to report pupil issues). Where such an incident may lead to significant harm, safeguarding procedures should be followed.

Complaints Regarding the Use of On-line Technology

Prompt action is required if a complaint is made. The facts of the case must be established and presented to the Computing Coordinator (who will inform the Headteacher/member of the SLT). A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the School’s Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Rochdale LA child protection procedures and our school policy.

Any complaints about staff misuse of on-line technology must be referred directly to the head teacher.

How to Respond When a Risk is Discovered

An inappropriate website is accessed inadvertently:

- You must report the website to the Computing lead and SLT and switch off the machine.
- Computing lead will then contact Remedian so that the site can be added to the banned or restricted list.
- Change Local Control filters to restrict locally.
- Log the incident.

An inappropriate website is accessed deliberately by an adult:

- Ensure that no one else can access the material (do not switch off the machine, the monitor can be switched off if applicable) and report to the Headteacher or Deputy Headteacher. Do not leave the machine unattended either bring it with you or ask another member of staff to inform the Headteacher.
- Log the incident.
- Report to the head and Computing Coordinator immediately.
- Head to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the filtering services in order to reassess the filters.

An inappropriate website is accessed deliberately by a child:

- Refer the child to the Acceptable use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Log the incident
- Decide on appropriate sanction.
- Notify the parent / carer.
- Contact the filtering service (Remedian) to notify them of the website.

An adult receives inappropriate material:

- Do not forward this material to anyone else even the HT or DSL– doing so could be an illegal activity. Material must be dealt with by police only.
- If received, try to minimise viewing of any innapropriate material i.e do not continue to view or try to investigate the material.
- Do not delete any images – all images must remain available for any necessary police investigation.
- Alert the Computing Coordinator, DSL and head teacher immediately.
- Ensure the device cannot be accessed by anyone and log the nature of the material.
- Contact relevant authorities for further advice e.g. police, social care, CEOP (Rochdale Sunrise Team).
- Log the incident.

An illegal website is accessed or illegal material is found on a computer.

The following incidents must be reported directly to the police.:

- Indecent images of children found. (Images of children whether they are photographs or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner).
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Criminally racist or anti-religious material.
- Software piracy.
- The promotion of illegal drug-taking.
- Adult material that potentially breaches the obscene publications act in the UK.

If any of these are found, the following should occur:

- DO NOT LOG OFF the computer, ensure nobody can access the device.
- Contact the police and or CEOP (Rochdale Sunrise Team) and social care immediately.
- Alert the Headteacher/ Designated Safety Lead.
- If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer.

An adult has communicated with a child or used ICT equipment inappropriately (e-mail/text message etc)

- Ensure the child is reassured and remove them from the situation.
- Report to Headteacher and DSL immediately, who will then follow the Allegations Procedure and Child Protection Procedures
- Report to the Local Authority Designated Officer.
- Preserve the information received by the child if possible.
- Contact the police as necessary.

Threatening or malicious comments are posted (or printed out) about an adult in school:

- Preserve any evidence and log the incident.
- Inform the Headteacher/Designated Safety Lead immediately who will then take any appropriate actions felt necessary.
- Contact the police or CEOP (Rochdale Sunrise Team) if appropriate.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Head teacher and Designated Safety Lead.

Threatening or malicious comments are posted about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

- Preserve any evidence and log the incident.
- Inform the Designated Safety Lead immediately and the Headteacher who will follow the Child Protection Policy.
- Check the filter if an internet based website issue.

- Contact/parents and carers
- Refer to the bullying policy
- Contact the police or CEOP (Rochdale Sunrise Team) as necessary.

Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum , Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives, understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

Use of Social Media

- Staff must ensure that they do not have any links to All Saints' school in their personal social media accounts.
- Staff are advised to ensure that all content on their social media accounts is set to private. All adults should review their social networking sites when they join the school to ensure that information and images that are available publicly are appropriate and could not cause offence or embarrassment.
- Staff should be made aware of the dangers of putting their personal information onto social networking sites such as their address, home or mobile phone number.
- Staff should consider content that they post and how this might be perceived.
- Staff should never make a friend of a pupil where they are working. They should seek advice from the Headteacher before becoming friends online with adult ex-students or parents. Staff should not be a friend of a pupil, parent or carer of a pupil or ex-pupil without seeking advice from the Headteacher.
- Staff should not access social networking pages of pupils.
- Staff must not request or respond to any personal information from a pupil or parent.
- Staff must not make comments on behalf of school or claim to represent the views of the school without explicit prior consent of the Head teacher.

Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular updates to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement.

Any organisation working with children and based on the school premises are required to sign the Acceptable Use Agreement.

Guidance is provided for occasional visitors, volunteers and parent/carer helpers on the 'Visitor and Supply Teacher information sheet.

Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.
It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and

associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Governors receive summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.