



E-Safety Policy

Next review: Autumn 2024

The purpose of this policy statement

St. Wilfrid's CofE Primary School works with children and families and this policy applies to all members of the school's community, including staff, pupils, parents and carers, volunteers and visitors. The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. The policy statement applies to all staff, volunteers, children and young people and anyone involved in the school's activities.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- Keeping children safe in education (KCSIE 2021)
- Working together to safeguard children (2018)
- Safeguarding and remote education during coronavirus (COVID-19) (2020)
- Teaching online safety in schools (2019)
- The Education People/Safeguarding/Online Safety
- Ofsted: Education Inspection Framework' 2021
- Early Years and Foundation Stage Framework 2021 (EYFS)
- The Education Act 2002
- www.nspcc.org.uk

Section 175 of the Education Act 2002 requires school governing bodies, local education authorities and further education institutions to make arrangements to safeguard and promote the welfare of all children who are pupils at a school, or who

St. Wilfrid's CofE Primary School

are students under 18 years of age. Such arrangements will have to have regard to any guidance issued by the Secretary of State.

This policy is one of a series in the school integrated safeguarding portfolio and should be read and actioned in conjunction with the policies as listed below:

- Behaviour management and use of physical intervention
- Code of conduct/Behaviour policy
- Online safety
- Social media
- Mobile and smart technology
- Anti-bullying
- Data protection and information sharing
- Image use
- Relationship and Sex Education (RSE)
- Personal and intimate care
- Attendance
- Risk assessments (e.g. school trips, use of technology)
- First aid and accidents
- Managing allegations against staff
- Staff behaviour policy/code of conduct, including Acceptable Use of Technology Policies (AUP)
- Safer recruitment
- Whistleblowing

Parents/carers can obtain a copy of the school's Child Protection Policy and other related policies on request. Additionally, our policies can be viewed via our website: <https://www.stwilfridsprimary.com/>

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online

St. Wilfrid's CofE Primary School

- we have a responsibility to help keep children and young people safe online, whether or not they are using our school's network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- the appointment of the Designated Safeguarding Lead (DSL)
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)

St. Wilfrid's CofE Primary School

- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term

The Role of the Designated Safeguarding Lead (DSL)

The school appoints the headteacher, as the Designated Safeguarding Lead (DSL). The DSL has overall responsibility for the day-to-day oversight of safeguarding and child protection systems (including online safety) in school. Whilst the activities of the DSL may be delegated to the deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL and this responsibility will not be delegated.

The DSL will undergo appropriate and specific training to provide them with the knowledge and skills required to carry out their role. Deputy DSLs will be trained to the same standard as the DSL. The DSLs training will be updated formally at least every two years, but their knowledge and skills will be updated through a variety of methods at regular intervals and at least annually.

The Role of The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their

St. Wilfrid's CofE Primary School

effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

Members of Staff

All members of staff have a responsibility to:

- Provide a safe environment in which children can learn.
- Be aware of the indicators of abuse and neglect so that they can identify cases of children who may need help or protection.
- Know what to do if a child tells them that he or she is being abused or neglected and understand the impact abuse and neglect can have upon a child.
- Be able to identify and act upon indicators that children are, or at risk of developing mental health issues.
- Be prepared to identify children who may benefit from early help.
- Understand the early help process and their role in it.
- Understand the school's safeguarding policies and systems.
- Undertake regular and appropriate training which is regularly updated.
- Be aware of the process of making referrals to children's social care and statutory assessment under the Children Act 1989.
- Know how to maintain an appropriate level of confidentiality.
- Reassure children who report concerns that they are being taken seriously and that they will be supported and kept safe.

Wi-fi

Pupils are not allowed networked access via personal devices. All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Volunteers, contractors, governors have no access to the school network or wireless internet on personal devices. Parents have no access to the school network or wireless internet on personal devices. All internet traffic is monitored.

St. Wilfrid's CofE Primary School

Email

Staff Email addresses and Class Dojo accounts are the only agreed means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern and should be notified to the DSL. Staff or pupil personal data should never be sent/shared/stored on email.

Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated has been the day-to-day responsibility of updating the content of the website to staff.

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

Office 365

Regarding pupils' Office 365 accounts, the school adheres to the principles of the DfE document '[Cloud computing services: guidance for school leaders, school staff and governing bodies](#)'.

The following principles apply:

- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such

St. Wilfrid's CofE Primary School

- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission

Only school-approved platforms are used by students or staff to store pupil work

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. No member of staff will ever use their personal phone to capture photos or videos of pupils (NB – many phones automatically back up photos).

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

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

Children and Young People

Children and young people (learners) have a right to:

- Feel safe, be listened to, and have their wishes and feelings taken into account.
- Confidently report abuse, knowing their concerns will be treated seriously, and knowing they can safely express their views and give feedback.
- Contribute to the development of safeguarding policies.
- Receive help from a trusted adult.
- Learn how to keep themselves safe, including online.

Pupils and parents should not be 'friends' with or make a friend request** to any staff, governors, volunteers via social media. (see staff code of conduct for more information)

St. Wilfrid's CofE Primary School

. Pupils and parents are discouraged from 'following' staff and governors' public accounts.

Mobile Phones

Pupils in Year 5 & 6 are allowed to bring mobile phones in for emergency use only, but not when moving around the school. During lessons, phones must remain turned off at all times. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to sanctions in line with the behaviour policy and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.

Parents and Carers

Parents/carers have a responsibility to:

- Understand and adhere the relevant school policies and procedures.
- Talk to their children about safeguarding issues with their children and support the school in their safeguarding approaches.
- Identify behaviours which could indicate that their child is at risk of harm including online.
- Seek help and support from the school or other agencies.

A partnership approach to online safety will support parents/carers to become aware and alert of the potential online benefits and risks for children by:

- Parent/carers signing up to an Acceptable Use agreement.
- Information and policies available on the school's website.
- Newsletters
- Safer Internet Day

Social Media

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into

St. Wilfrid's CofE Primary School

disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

Many social media platforms have a minimum age of 13, or even 16. However, the school occasionally deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

The school acknowledges that in order to best help our pupils/students to avoid or cope with social media issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Recording Concerns

- All safeguarding concerns, discussions and decisions, and reasons for those decisions, will be recorded in writing and passed without delay to the DSL.
- Records will be completed as soon as possible after the incident/event, using the child's words and will be signed and dated by the member of staff. Child protection records will record facts and not personal opinions.
- If there is an immediate safeguarding concern the member of staff will consult with a DSL before completing the form as reporting urgent concerns takes priority.
- If members of staff are in any doubt about recording requirements, they will discuss their concerns with the DSL.
- In addition to the child protection file, the DSL will also consider if it would be appropriate to share any information with the DSL at the new school or college in advance of a child leaving, for example, information that would allow the new school or college to continue to provide support.

Where the school receives child protection files, the DSL will ensure key staff such as the special educational needs co-ordinators (SENCOs), will be made aware of relevant information as required.

St. Wilfrid's CofE Primary School

Confidentiality and Information Sharing

- The School recognises our duty and powers to hold, use and share relevant information with appropriate agencies in matters relating to child protection at the earliest opportunity as per statutory guidance outlined within KCSIE 2021.
- St Wilfrid's CofE Primary School has an appropriately trained Data Protection Officer (DPO) as required by the General Data Protection Regulations (GDPR) to ensure that our school is compliant with all matters relating to confidentiality and information sharing requirements.
- The headteacher and DSL will disclose relevant safeguarding information about a learner with staff on a 'need to know' basis.
- All members of staff must be aware that whilst they have duties to keep information confidential, in line with our confidentiality policy, they also have a professional responsibility to be proactive in sharing information as early as possible to help identify, assess, and respond to risks or concerns about the safety and welfare of children; this may include sharing information with the DSL and with other agencies as appropriate. All staff are aware they cannot promise confidentiality in situations which might compromise a child's safety or wellbeing.

Complaints

- All members of the school community should feel able to raise or report any concerns about children's safety or potential failures in the school safeguarding regime. The school has a complaints procedure available to parents, learners and members of staff and visitors who wish to report concerns or complaints, available upon request.
- Whilst we encourage members of our community to report concerns and complaints directly to us, we recognise this may not always be possible. Children, young people, and adults who have experienced abuse at school can contact the NSPCC 'Report Abuse in Education' helpline on 0800 136 663 or via email: help@nspcc.org.uk
- Staff can also access the NSPCC whistleblowing helpline if they do not feel able to raise concerns regarding child protection failures internally.
- Staff can call 0800 028 0285 (8:00 AM to 8:00 PM Monday to Friday) or email help@nspcc.org.uk.

St. Wilfrid's CofE Primary School

- The leadership team will take all concerns reported to the school seriously and all complaints will be considered and responded to in line with the relevant and appropriate process.

Anything that constitutes an allegation against a member of staff or volunteer will be dealt with in line with section 8 of this policy.

Safeguarding Issues

The school is aware of a range of specific safeguarding issues and situations that can put children at greater risk of harm. It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. St. Wilfrid's adopts a whole school approach to online safety which will empower, protect, and educate our learners and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful content. For example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users. For example peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Technology, and the risks and harms related to it, evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment which considers and reflects the risks our children face.

The Headteacher/DSL will be informed of online safety concerns, as appropriate. The DSL has overall responsibility for online safety within the school but will liaise with other members of staff, for example IT technicians, curriculum leads etc. as necessary.

The DSL will respond to online safety concerns reported in line with our child protection and other associated policies, including our anti-bullying, behaviour policies.

- Internal sanctions and/or support will be implemented as appropriate.

St. Wilfrid's CofE Primary School

- Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

The school uses a wide range of technology. This includes computers, laptops, tablets and other digital devices, the internet, apps and email systems.

- All school owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

The school recognises the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras and wearable technology. In accordance with KCSIE 2021 and EYFS 2021. Appropriate mobile and smart technology and image use policies are in place, and are shared and understood by all members of the community.

Appropriate Filtering and Monitoring

The school will do all we reasonably can to limit children's exposure to online risks through school provided IT systems and will ensure that appropriate filtering and monitoring systems are in place.

Whilst filtering and monitoring is an important part of school online safety responsibilities, it is only one part of our approach to online safety.

- Learners internet use, search tools and apps will be supervised by staff according to their age and ability.
- Learners will be directed to use age appropriate online resources and tools by staff.

The school will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Staff Training

All staff will receive online safety training as part of induction and that ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.

Remote Learning

Specific guidance for DSLs and SLT regarding remote learning is available at DfE: Safeguarding and remote education during coronavirus (COVID-19) and The Education People: Remote Learning Guidance for SLT.

St. Wilfrid's CofE Primary School

Staff will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.

All communication with learners and parents/carers will take place using provided or approved communication channels; for example, provided email accounts and phone numbers as well agreed systems e.g. Google Classroom, Microsoft 365 or equivalent.

Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our school and Acceptable Use Policies.

Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.

When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP).

Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. The school will continue to be clear who from the school their child is going to be interacting with online.

Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

Trips

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils and parents. Where this is not possible, they may use their own phone if necessary, with permission from the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

St. Wilfrid's CofE Primary School

However, in such circumstances, staff are strongly advised to speak to the Headteacher for further advice before any search is undertaken.