

Guilden Sutton Church of England Primary School



'Love and Justice for All'

'And what does the Lord require of you? To act justly and to love mercy and to walk humbly with your God.' Micah 6:8.

through the teachings of Jesus all can flourish spiritually, emotionally and academically throughout life, living out love and justice for all.

E-Safety Policy

Staff member responsible	Mrs. T. Rainford
Governor/Other responsible	Mrs. J. Hawkins
Date of Policy	December 2025
Reviewed	3-5 years

Policy for Online Safety and Acceptable Usage

- Explanation of text
- Physical Safety
- Network Safety
- Internet Safety
- E-mail Safety
- Cross Curricular Links
- Use of Digital Images
- E-Bullying
- Mobile Phones
- Other Technologies
- Copyright
- Data Protection Act
- Online Safety Rules
- Prevent Training

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Guilden Sutton Church of England Primary School, we recognise that learning is a lifelong process and that e-learning is an integral part of it.

Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Online safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy clearly sets out our expectations of pupils, staff, parents and members of the wider community to ensure best practice.

Key:

Normal text gives contexts and information

Italic text indicates teaching given to pupils

Bold text indicates key expectation to ensure positive and safe use

Physical Safety:

- Liquids can be damaging and pose a fire risks when in contact with electrical equipment. *Pupils are taught to avoid taking liquids anywhere near the computers. We expect all users to refrain from drinking when working at a computer.*
- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. *Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy. We expect all users to take responsibility for their own physical well-being by adopting good practices.*
- Computers and other ICT equipment can be easily damaged. *Pupils are taught the correct way to carry and use ICT equipment. We expect pupils to respect ICT equipment and take care when handling and using.*

Network Safety:

- All users need to log on using a username and password. *Pupils are taught that they should access the network using only those login details. We expect all users to only log on using their username.*
- Each user is given an allocated, named folder on the school 'Work Share' area of the network for the storage of their work. *Pupils are taught how to save their work into their own area within 'Work Share'. We expect pupils to save and keep their work to build up a portfolio of evidence, where work that they are proud of can be viewed and shared as good practice across year groups. Children are taught not to delete or alter others' work and to ensure that they only save work to shared areas with permission.*
- On the network there are "shared resource" areas where many different groups of users can save work so that it is available to others. *Pupils are taught how to access and save to these shared resource areas. We expect pupils to respect the contributions of others,*

not to delete or alter others' work and to ensure that they only save work to shared areas with permission.

- *Pupils are taught to only print when necessary to save resources for financial and environmental reasons. We expect pupils to only print out work when directed by staff to do so.*
- The network software prevents changes being made to computer settings. *Pupils are taught that making changes may prevent the computer from working properly. We expect all users to make no attempt to alter the way the computer is set up.*
- Only the network administrators are permitted to install software on to computers. *Pupils are taught that the network or an application may not function properly if programmes are installed. We expect all users to make no attempt to load or download any programme onto the network.*
- All users of the network can be monitored remotely by the network administrators. *Pupils are taught that their use of the network can be monitored. We expect all users to understand that their use is subject to monitoring.*

Passwords:

Protecting access to school-related online accounts is essential to maintaining a safe digital environment for all staff and pupils. One of the simplest ways for a cybercriminal to gain unauthorised access is through weak or reused passwords. Fraudsters may also use advanced tools, including Artificial Intelligence (AI), to guess or regenerate passwords. By following the guidance below, all members of the school community can significantly reduce the risk of such breaches.

To help protect your online accounts:

- **Never reuse passwords across different accounts. Each account should have its own unique password.**
- **Create complex and unique passwords that are difficult to guess. Avoid using personal information such as names, birthdays, or simple patterns.**
- **Enable Two-Factor Authentication (2FA) wherever possible. This provides an extra layer of protection even if your password becomes compromised.** Two-Factor Authentication is needed for members of staff to access their staff email accounts.
- **Use a reputable Password Manager to securely store and manage your passwords.**
- **Check periodically to see if your passwords have been lost during a Cyber Data attack on a company that you have shared your password with.**

By following these practices, staff, pupils, and parents can help safeguard the school's digital systems and personal information from unauthorised access.

Internet Safety:

- When using a network workstation, all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. Half termly reports are produced on the effectiveness of the filtering system using 'testfiltering.com' and any issues are reported to the network administrators. However, no system is 100% safe and we expect users to behave responsibly. *Pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your computer.* **We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media, and to report any unsuitable material to staff immediately.**
- Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. **We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.**
- The school website contains school policies, newsletters and other information. **We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.**
- Pupils and parents are given access to the school website/learning platform through a username and password. **We expect parents and pupils to be respectful when making comments and adding text/images or videos to the learning platform. They should only upload work which is suitable for school use.**

Digital Images:

- Digital images and videos are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. On the website we never state a child's full name with their image. **The school will happily remove any image of a child on the school website at their parent's request.**
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. All such use is monitored and supervised by staff. *Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within school.* **We**

expect all pupils to seek permission from staff before sharing images outside of the school environment.

E-Bullying:

- The school takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any digital communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. *Pupils are taught about bullying as part of the whole school curriculum, with a particular focus during P.S.H.E. sessions that are linked to our Coram Life Education scheme of work. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policy on Behaviour, including bullying.*

Mobile Phones:

- Pupils are not permitted to have mobile phones upon their person in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However, we discourage this on security grounds as they are easily lost, damaged or stolen. *Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the office for the duration of the day. We expect pupils not to carry a mobile phone in school.*

Sexting:

- 'Sexting' is considered by many to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet.' Yet when young people are asked 'What does sexting mean to you?' they are more likely to interpret sexting as 'writing and sharing explicit messages with people they know'. Similarly, many parents think of sexting as flirty or sexual text messages rather than images.
- On this basis, current advice introduces the phrase 'youth produced sexual imagery' and uses this instead of 'sexting.' This is to ensure clarity about the issues current advice addresses.

'Youth produced sexual imagery' best describes the practice because:

- 'Youth produced' includes young people sharing images that they, or another young person, have created of themselves.
- 'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context.
- 'Imagery' covers both still photos and moving videos (and this is what is meant by reference to imagery throughout the document).

The types of incidents which this covers are:

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18

- Any involvement in 'youth produced sexual imagery' is illegal and strictly forbidden by any member of the school community.
- If an incident should occur then staff are advised to follow the advice given here:
[https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545997/Sexting in schools and colleges UKCCIS 4.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545997/Sexting_in_schools_and_colleges_UKCCIS_4.pdf)

Copyright:

- Although there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances; this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. *Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission. We expect all users to respect copyright laws.*

Data Protection Act:

- The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from the Department of Constitutional Affairs – www.justice.gov.uk

Use of Artificial Intelligence (AI):

- At Guilden Sutton Church of England Primary School, we acknowledge the potential of artificial intelligence (AI) to enhance learning, ease teacher workload and equip pupils for how emerging technologies will change workplaces. The school aims to ensure that AI is

used effectively, safely and appropriately to deliver excellent education that prepares our pupils to contribute to society and the future workplace

- By teaching responsible AI usage, we provide a knowledge-rich curriculum that helps pupils become informed, critical users of technology while understanding its societal impact. They will be guided in selecting suitable resources, including AI tools where appropriate, to support their learning without becoming overly dependent on a limited range of technologies.

Glossary of Terms

- **Email** Text based messages sent through the Internet
- **Internet** A global network of computers which allow efficient communication from any point to any point
- **Network** A group of computers linked together and often managed by a server
- **Podcast** One of a series of sound files uploaded on to the Internet and download by subscribers
- **Server** A computer that controls access to a network of computers and usually stores data for all users
- **Webmail** Email service which is held on a secure website and can be accessed anywhere on the Internet
- **Artificial Intelligence (AI)** Technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

Online Safety Rules for Pupils

‘Think then click’

- We ask permission before using the Internet.
- We only use suitable websites for research.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we not sure about.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not use Internet chat rooms.

Prevent Training

As part of Guilden Sutton Church of England Primary School's on-going safeguarding and child protection duties, we are fully behind the government's *Prevent Strategy*.

From 1 July 2015, all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”. This duty is known as the *Prevent Duty for Schools*.

At Guilden Sutton Church of England Primary School, we build pupils' resilience to radicalisation by promoting fundamental British values and enabling our pupils to challenge extremist views. You can read about what we do to promote British values on our website.

The statutory guidance refers to the importance of *Prevent* awareness training to equip staff to identify children at risk of being drawn into terrorism and to challenge extremist ideas. The Home Office has developed a core training product for this purpose – Workshop to Raise Awareness of Prevent (WRAP). All governors and staff have received WRAP training sessions on what *Prevent* is about and how to deal with any issues they may see inside or outside school.

Social Media

Guilden Sutton Church of England Primary School's social media accounts are used and followed principally by staff, parents and other professionals in order to advertise the excellent work by staff, pupils, parents and governors and to celebrate the success and achievements of the children. Similarly, they also contain information detailing specific events in school. Whilst using social media, all staff demonstrate safe and responsible usage.

We use social media to **SCIPPE (Share, Celebrate, Inform, Promote, Publicise and Engage) with our school community and the wider community.**

Our social media content reflects the 'school voice' - the ethos, attitudes and values of the school.

- **Pupil safety and safeguarding will always be a central consideration. No full names are used alongside photos of individual children or small groups. Certain children must not appear in the press, on open websites or in other forms of media which may allow estranged parents, birth parents etc. to locate the child. These children are identified using the GDPR form sent to parents when their child joins school.**
- We use social media as an 'information channel' to share the great range of activities that happen in school, such as themed weeks, competitions, visitors and day-to-day learning.
- We aim to maintain a balance of news from a range of subjects and year groups, and avoid posting photographs of the same children frequently.

The content of our social media channels is monitored by a selection of approved staff. They alone are responsible for password protection and following of other users. Posts will primarily be shared between the hours of 8am and 8pm between Monday and Friday, although other key messages and reminders may be shared outside these times.

Inappropriate content and referencing

Guilden Sutton Church of England Primary School welcomes any referencing, mentions, or interactions that post the school in a positive light only. Therefore, the school deems any of the following as inappropriate:

- Offensive language or remarks aimed at the school, its staff, parents, governors or others affiliated with the school.
- Unsuitable images or content posted into its feed.
- Images or text that infringe upon copyright.
- Comments that aim to undermine the school, its staff, parents, governors or others affiliated with the school. Any inappropriate content will be deleted and its users will be removed, blocked, and, depending on the nature of the comment, reported to Twitter and Facebook. Furthermore, incidents of a more serious nature may be reported to the appropriate authority.