Witley C of E Infant School

Learn, love and flourish together

Online Safety Policy

Status of document	
Document type	Non-statutory
Date last reviewed	June 2024
Date reviewed	November 2025
Reviewed by	FGB
Date next review	November 2026
Review cycle	Annual
Available on website	Yes
Approval level	Full governing Body

Overview

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, data handling and the use of images.

- The online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication at school, between school and home and home learning. This includes but is not limited to workstations, laptops, mobile phones, tablets and Chromebooks.

- The online safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Witley C of E Infant School Online Safety Policy

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, governors and anyone involved in our school activities.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- To ensure that appropriate filters and monitoring systems are in place to protect children when they are online on the school IT systems or using resources recommended for parents during home learning.

Legislation and guidance

This policy is based on the following DfE's statutory safeguarding guidance, and its advice and guidance for schools:

Preventing and Tackling Bullying
Searching, screening and confiscation
Keeping Children Safe in Education
Teaching Online Safety in School (2023)
Protecting children from radicalisation

This policy also takes into account the National Curriculum computing programmes of study and Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance documents.

The 4Cs

Being online can be a great source of fun, entertainment, communication and education. Some people's online behaviour places others at risk. The number of issues covered under online safety is large and constantly growing. Witley C of E Infant School takes into account the 4Cs when ensuring online safety. The risks are categorised into these four areas:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism misinformation, disinformation (including fake news) and conspiracy theories.

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 children for sexual, criminal, financial or other purposes.

Conduct: 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. If children or members of staff report any issues, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam and malware protection and such safety mechanisms are updated regularly.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security and monitoring of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

The school will provide an age-appropriate online safety curriculum, which is currently Project Evolve, that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. This shall be embedded as a whole school approach. All communication between staff and pupils or families will take place only using school accounts.

Pupils will be taught to use technology safely and respectfully, keeping information private. They shall be taught not to give out personal details or information which may identify them or their location. Children are taught to only use 'safe' search engines that have been identified. Children will be taught the importance of principles of positive relationships online in line with the Relationships Education, Relationships and Sex Education (RSE) and Health Education curriculum. Teaching will include how information and data is shared and used.

Through the physical health and well-being curriculum coverage, pupils will be taught about the benefits of rationing time spent online and the risk of excessive use of electronic devices.

As part of the Relationships Education, Relationships and Sex Education and Health Education curriculum, pupils will gain knowledge of how to critically consider sources of information. Pupils will be taught how to distinguish fact from opinion, as well as exploring freedom of speech and the role of media in informing and shaping public opinion. The school will emphasise the teaching of democracy, freedom, rights and responsibilities. Pupils will be taught how to evaluate what they see online and enable them to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Pupils will be taught, through PSHE lessons, where to go for help and support when they have concerns about the content or contact on the internet or other online technologies.

During any future school closure or partial closure:

- It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per our Safeguarding and Child Protection Policy.

- Online teaching should follow the same principles as set out in the School code of conduct.
- Witley School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
- The school will send online work to pupils via our secure Google Classroom.
- If whole class or whole school lockdown should arise the school will provide continuous learning via Google Classroom and Google Meet.

The following guidelines are in place for parents/carers, who are asked to read and comply with them in the context of online home learning:

Online Home Learning Guidelines for Parents and Carers

- Make sure your child understands and is aware of the pupil guidelines
- Answer the phone to school staff or return calls, messages or emails. Staff may call from a withheld number
- Supervise your child's internet use and online learning – make sure you are aware of what they have been asked to do and the websites they need to access.
- Make sure you know who your child is talking to or messaging.
- If a member of staff calls to speak to your children – check that you know who they are, speak to the member of staff yourself before your child talks to them, stay in the room while your child is on the phone.
- Monthly Online Safety newsletters are emailed to all parents/carers keeping them up to date with current technology issues i.e. age appropriate gaming/Apps
- Parental Controls booklet is emailed at least one a year to parents/carers to support online safety at home.

Guidelines for All Google Meet Video lessons

- The parent or carer must make sure their child and other members of the household are aware the video call is happening.
- Staff, children and other members of the household must wear suitable clothing
- Devices used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background. Language must be professional and appropriate, including any family members in the background.
- The same expectations apply for remote teaching and conversations as normal school conduct
- Staff will only ever video call a pupil with prior agreement with parents and the head teacher or deputy. This will always be at a pre-arranged time. The times of all video calls and lessons will be notified to you in advance.
- Parents will need to appear on screen at the start of the lesson to confirm they give consent for their child to be part of the group conversation.

Group Google Meet Video Lessons

- These will be group conversations only.
- If your child takes part in a group video conversation, they can be seen by the teacher and other pupils (and members of their household) that are part of the conversation.
- Parents will need to give consent for their child to be part of a group video lesson.
- Parents will need to appear on screen at the start of the lesson to confirm they give consent for their child to be part of the group conversation.
- If the teacher has any concerns about children (or other members of the household) using unsuitable language, dress, location, the conversation will be ended and concerns will be recorded and passed to the head teacher.
- Live classes should be kept to a reasonable length of time and should take place during normal

lesson times.

1:1 Video Conversations:

- Staff will only ever video call a pupil with prior agreement with parents and the head teacher or deputy. This will be at a pre-arranged time and day.
- The staff member will speak first with the parent or carer to check they are aware of the call. The parent or carer must stay in the room.

Witley School staff will be in regular communications with parents and carers and will reinforce the importance of children being safe online.

Witley School staff will continue to support parents and carers by sharing and recommending support websites containing information about keeping their child safe online. These include:

- Internet matters - for support for parents and carers to keep their children safe online
- London Grid for Learning - for support for parents and carers to keep their children safe online
- Net-aware - for support for parents and careers from the NSPCC
- Parent info - for support for parents and carers to keep their children safe online
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers.

E-mail use

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil communication must only take place via Google Classroom.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Published content (e.g. school website, school social media accounts)

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or person nominated by the headteacher will take overall editorial responsibility and ensure that content isaccurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media account as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreyscb.org.uk/

Use of social media

- Staff and pupils should ensure that their online activity, both in school and out, takes into account the feelings of others and is appropriate for their situation as a member of the school community.
- Through IT lessons, children will be taught how to keep themselves safe online. Age appropriate resources and literature will be used.

- Through Relationships Education (and RSE), teaching will give pupils the knowledge they need to recognise and to report abuse, including emotional and sexual abuse. This will be delivered by focusing on boundaries and privacy, ensuring pupils understand that they have rights over their own bodies. Pupils will also be taught understanding boundaries in friendships with peers and also in families and with others, in all contexts, including online.

Use of personal devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the online safety policy and the relevant AUP (Acceptable Use Policy).
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.
- Personal devices of both staff, governors and visitors, such as mobile phones, tablets will be stored away in handbags and not used around children during the school day. Detailed guidance can be found in our Staff Code of Conduct.

Protecting personal data

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians, governors and visitors) must read and sign the 'Staff AUTP' (Acceptable Use of ICT Policy) before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- Access to the internet for pupils will be by adult demonstration with supervised access to specific, approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access.

Handling online safety complaints

- Complaints of internet misuse will be dealt according to the school Behaviour Policy and Staff Code of Conduct Policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. These are set out in full in our Safeguarding and Child Protection Policy.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' Positive Behaviour Policy.
- Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with staff disciplinary procedures. The school will consider whether incidences which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is (in an age appropriate manner), and what to do if they become aware of it happening to them or others. We will ensure pupils know how they can report any incidents and are encouraged to do so,

including where they are a witness rather than the victim.

- Through the Relationships Education (RSE) curriculum, pupils will be taught that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others including when we are anonymous. Pupils will be taught that sometimes people behave differently online, including pretending to be someone they are not.
- Complaints of cyber-bullying will be dealt with according to the school Behaviour and Anti-bullying Policy and parents will be informed.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Pupil mobile phones and smart technology (including smart watches)

- Many children have unlimited and unrestricted access to the internet via mobile phone networks; therefore children could be harmed or harm others online when at school. This may include sexually harassing, bullying and sharing indecent images (often via large chat groups).
- To protect children from these risks while they are at our school, our school does not allow pupils to bring mobile phones or smart watches onto the premises and therefore pupils are prohibited from using them in school.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the pupil AUP (acceptable use policy) in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the AUP as part of their online safety education termly.
- Pupils considered at risk will be provided with appropriate and differentiated online safety education.

To staff

- All staff will be shown where to access the online safety policy and its importance explained.
- All new staff will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff will receive online safety training on an annual basis and receive regular updates regardingchanges and guidance or emerging online safety concerns.

To parents

- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters, the school brochure and on the school website. Links supporting guidance on keeping children safe online will be available on the school website.

- The school will raise parent awareness of internet safety by offering online safety training annually through parent information evenings and providing lists of supporting organisations/resourceson the school website.
- If parents have concerns or queries in relation to online safety, these should be raised in the first instance with the Headteacher/DSL.
- Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

To Governors

- The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, filtering and monitoring and monitor the online safety log as provided by the designated safety lead (DSL).
- Governors will agree and adhere to the terms of acceptance of use of the school ICT systems and the internet.

Monitoring

The DSL logs behaviour and safeguarding issues related to online safety through CPOMS, our online reporting system.

End of policy.