

Whittington Church of Online Safety Policy



To love, to learn, to flourish - together

School Vision

Jesus said, 'I chose you and appointed you to bear much fruit, fruit that will last.' John 15:16

We are inspired by Jesus to learn with joy and flourish in love, faith and wisdom. Together, we live and grow well, valuing and respecting our differences and sharing our God given gifts. We aspire to be courageous and responsible, caring for our world and one another today for a better tomorrow.

Policy adopted: Sept 24

Policy review: Sept 25

Contents:

Statement of intent

1. Teaching and learning
2. Managing internet access
3. Policy decisions
4. Pupil online safety curriculum
5. Communications policy

Appendix

1. Staff, Governor and Visitor Acceptable Use Agreement
2. Acceptable Use Agreement

Statement of intent

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 4/5G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

Online safety is a child protection issue, and indeed it should not be managed primarily by the Computing team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of Computing-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

Teaching and learning

Why the internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. As a school, we have a duty to provide pupils with quality internet access as part of their learning experience and to support the statutory curriculum.

At Whittington, teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas. Pupils are taught how to use the internet appropriately and safely and how they can present their findings to others using a variety of different software. They are taught the importance of cross-checking information before accepting its accuracy and how to report any unpleasant

internet content to their class teacher or teaching assistant. This can be done in person and will be treated in confidence.

The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience. The programs include:

- Google Be Internet Legends
- Childnet
- CEOP

Managing internet access

Information system security

1.1. School ICT systems security is reviewed regularly.

1.2. Virus protection is updated regularly.

1.3. Any security updates suggested by the Local Authority will be implemented by the school Email

1.4. The school:

- Provides staff with an email account for their professional use (Office 365) and makes clear any personal emails should be through a separate account.
- Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

Published content and the school website

1.5 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

1.6 Staff or pupil personal contact information will not be published. The contact details given online are of the school office.

1.7 The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

1.8 Uploading of information is restricted to our website authorisers.

1.9 The school website complies with the following statutory DfE guidelines for publications:

- What maintained schools must publish online

1.10 Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

1.11 Photographs published on the web do not have full names attached.

1.12 The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Publishing pupils' images and work

- 1.13 Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. The school will consider using group photographs rather than full-face photos of individual children.
- 1.14 Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
- 1.15 Written permission from parents will be obtained before photographs of pupils are published on the school website.
- 1.16 Pupil image file names will not refer to the pupil by name.
- 1.17 Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- 1.18 The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.
- 1.19 The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- 1.20 Staff sign the read and agree to this acceptable use policy as well as reading and agreeing the 'Staff Behaviour policy'. Both policies set out how staff members conduct themselves through digital technologies.
- 1.21 Pupils are taught about how images can be manipulated in their online safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- 1.22 Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- 1.23 Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images, that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social networking and personal publishing

- 1.24 The school will control access to social networking sites and consider how to educate pupils in their safe use.
- 1.25 Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

1.26 Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

1.27 Pupils will be advised to use nicknames and avatars when using social networking sites.

1.28 Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.

1.29 Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school's preferred system for such communications.

1.30 School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.

Managing filtering

1.31 If staff or pupils come across unsuitable online materials, the site must be reported to the Head teacher.

1.32 Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing and webcam use

1.33 Videoconferencing should use the educational broadband network to ensure quality of service and security.

1.34 Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

1.35 Videoconferencing and webcam use will be appropriately supervised.

Class Dojo

1.5. The school gains parental permission from all parents before signing up to use Class Dojo.

1.6. Photographs that include pupils are selected before being uploaded to Class Dojo so that only pupils where consent has been given will have their image uploaded.

1.7. Private messages to parents via Class Dojo will not contain any confidential or personal information about staff, pupils or their families. Any messages that may be deemed as inappropriate or of concern will be passed on to the Head teacher.

Protecting personal data

- 1.36 Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

Personal devices and mobile phones

- 1.37 The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded.
- 1.38 Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- 1.39 Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times.
- 1.40 Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- 1.41 No images or videos are taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- 1.42 Staff handheld devices, including i-pads and personal cameras, must be noted in school – name, make and model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school.
- 1.43 Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- 1.44 Staff will not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- 1.45 If a member of staff breaches the school policy, disciplinary action may be taken.
- 1.46 Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- 1.47 Pupils will abide by the following rules when using personal devices in school:

- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parents in accordance with the school policy.
- If a pupil needs to contact their parents, they will be allowed to use a school phone.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No pupil should bring their mobile phone or personally-owned device into school. Any device brought into school without permission will be confiscated.

2 Policy decisions

Authorising internet access

- 2.5 All staff will read and sign the [Staff, Governor and Visitor Acceptable Use Agreement](#) before using any school ICT resource.
- 2.6 The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- 2.7 At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- 2.8 Any person not directly employed by the school will be asked to sign the [Staff, Governor and Visitor Acceptable Use Agreement](#) before being allowed to access the internet from the school site.

Assessing risks

- 2.9 The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.
- 2.10 The school should audit ICT use to establish if the Online safety Policy is adequate and that the implementation of the Online safety Policy is appropriate and effective.

Handling online safety complaints

- 2.11 Complaints of internet misuse will be dealt with by a senior member of staff.
- 2.12 Any complaint about staff misuse must be referred to the Head teacher.
- 2.13 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- 2.14 Pupils and parents will be informed of the consequences for pupils misusing the internet.

3 Pupil online safety curriculum

Teaching and learning

3.5 This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, this includes:

- Google Be Internet Legends
- Childnet
- CEOP

3.6 Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

3.7 The school will remind pupils about their responsibilities through a [Pupil Acceptable Use Agreement](#) which every pupil will sign.

3.8 All staff will model safe and responsible behaviour in their own use of technology during lessons.

Online risks

3.9 The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE and Computing) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

3.10 Cyber bullying can be defined as “Any form of bullying which takes place online or through smartphones and tablets.” - BullyingUK

3.11 Complaints of online bullying are dealt with in accordance with our ‘Behaviour Policy’. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

3.12 Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

3.13 Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

3.14 All incidents of cyber bullying reported to the school will be recorded.

4 Communications policy

Introducing the Online safety Policy to pupils

4.5 Pupils are regularly reminded of the Online safety rules and guidance within school.

4.6 Pupils will be informed that network and internet use will be monitored and appropriately followed up.

4.7 Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.



Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the Head teacher.

- I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head teacher or governing board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system and mobile devices for any communications with pupils, parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the Head teacher or governing board and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the Head teacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member.

Images will not be distributed outside the school network without the permission of the parent, member of staff or Head teacher in line with data security policy.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the school's Online safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature _____

Date _____

Full name _____ (Printed)



Pupil Acceptable Use Agreement

At Whittington, we use technology in a variety of ways to support and enhance the curriculum we provide. When using a computer or any other new technology at school it is important that all pupils feel safe and know what is expected of their behaviour. This acceptable use agreement will help you understand how to keep safe when using technology and where to go for help.

When I am using school equipment I agree to do the following:

- I will only use technology, such as a computer or tablet, when a teacher has given me permission.
- I will only use technology and the internet for the reasons outlined by my teacher.
- I will look after the device and not damage it.
- I will tell a teacher if I see something that makes me upset or uncomfortable.
- I will keep my passwords secret and not share any personal information online (e.g. date of birth, address, school).
- I will not speak to anyone I do not know on the internet.

I also understand that school has the right to take action if I am involved in incidents of inappropriate behaviour when I am out of school if they involve the school community (e.g. cyberbullying, inappropriate use of images, posting inappropriate or untrue comments onto websites or social media which mention the school community) or if I use my own technology in school (e.g. mobile phone).

Signature _____

Date _____

Full name _____ (Printed)