WICKLEWOOD PRIMARY SCHOOL AND NURSERY

ONLINE SAFETY POLICY

Responsible Person

The appropriate responsible person for the updating of this policy is: **The Headteacher**

Review and Monitoring:

This policy will be reviewed every year.

Reviewed:

Next Review due:

Reviewed by:

This policy was approved by Governing Board on 07/12/2022

Statement of intent

At Wicklewood Primary School and Nursery, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1. Legal framework

1.1. This policy has due regard to all relevant legislation including, but not limited to:

- The Data Protection Act 2018 (GDPR)
- Freedom of Information Act 2000.

1.2. This policy also has regard to the following statutory guidance:

- DfE (2022) 'Keeping children safe in education'.

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Safeguarding Policy, including Child Protection
- Anti-bullying Policy
- Online Safety Acceptable Use Agreements
- Computing Policy
- Staff Code of Practice
- Mobile Phone Policy

- Staff Code of Conduct.

1.4 This policy will be used in conjunction with the DfE 'Teaching Online Safety in School' June 2019.

2. Use of the internet

2.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:

- access to illegal, harmful or inappropriate images;
- cyber bullying;
- access to, or loss of, personal information;
- access to unsuitable online videos or games;
- loss of personal images;
- inappropriate communication with others;
- illegal downloading of files;
- exposure to explicit or harmful content, e.g. involving radicalisation;
- plagiarism and copyright infringement;
- sharing the personal information of others without the individual's consent or knowledge.

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The governing board is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

3.3. The headteacher is responsible for ensuring the day-to-day online safety in the school and managing any issues that may arise.

3.4. The headteacher is responsible for ensuring that staff receive CPD to allow them to fulfil their role.

3.5. The computing coordinator will provide advice for members of staff as part of the requirement for them to be able to teach pupils about online safety.

3.6. The headteacher and computing coordinator will carry out the monitoring of online safety in the school, keeping in mind data protection requirements.

3.7. The headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.8. The headteacher will ensure that all members of staff are aware of the procedure when reporting online safety incidents and teachers will keep a record of all incidents on CPOMS (Child Protection Online Monitoring and Safeguarding system).

3.9. The governing board will hold meetings with the headteacher to discuss the effectiveness of the online safety provision, current issues, and to review incident logs, as part of the school's duty of care (Safeguarding).

3.10. The governing board will evaluate and review this Online Safety Policy on a annual basis, considering the latest developments in ICT and the feedback from staff/pupils.

3.11. The headteacher will review and amend this policy with the computing coordinator, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.12. Teachers are responsible for ensuring that online safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.13. All staff are responsible for ensuring they are up-to-date with current online safety issues, and this Online Safety Policy.

3.14. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the headteacher.

3.15. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.16. The headteacher is responsible for communicating with parents regularly and updating them on current online safety issues and control measures.

3.17. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. Online safety education

Educating pupils:

4.1. An online safety programme is established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

4.2. Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

4.3. Clear guidance on the rules of internet use will be presented in all classrooms in an age appropriate manner.

4.4. Pupils are instructed to report any suspicious use of the internet and digital devices to their classroom teacher.

4.5. PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help at an age appropriate level.

4.6. The school may hold online safety events, such as Safer Internet Day and Friendship Week, to promote online safety.

Educating staff:

4.7. All staff will undergo online safety training to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media and the internet as a whole.

4.8. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.9. All new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this Online Safety Policy.

4.10. The computing curriculum lead will act as the first point of contact for staff requiring online safety advice.

Educating parents:

4.11. Online safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.

4.12. Twilight courses and presentations may be run by the school for parents.

4.13. Learning reviews, meetings and other similar occasions may be utilised to inform parents of any online safety related concerns.

5. Online safety control measures

Internet access:

5.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.

5.2. A record will be kept by the office staff / teachers of all pupils who have been granted internet access.

5.3. Where possible all users in KS2 and above will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.

5.4. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.5. Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

5.6. The governing board will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

5.7. All school systems will be protected by up-to-date virus software.

5.8. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

5.9. Staff are only able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

5.10. Personal use will only be monitored by the headteacher for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

5.11. Inappropriate internet access by staff will be dealt with following the procedures outlined in the misuse by staff section of this policy.

Email:

5.12. Staff will be given approved email accounts and are only able to use these accounts. This provision may be extended to pupils for teaching purposes.

5.13. The use of personal email accounts to send and receive personal data or information is prohibited.

5.14. No sensitive personal data shall be sent to any other pupils, staff or third parties via email.

5.15. Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.

5.16. Staff members are aware that their email messages may be monitored.

5.17. Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.

5.18. Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.19. Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future – the headteacher will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

5.20. Pupils will not have access to social networking sites at school. Access to social networking sites will be filtered as appropriate.

5.21. Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.

5.22. Pupils are regularly educated on the implications of posting personal data online outside of the school.

5.23. Pupils or parents must not place personal photos on any social network space provided by the school, eg. the school's Facebook page.

5.24. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

5.25. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

5.26. Staff are not permitted to publish comments about the school which may affect its reputability.

5.27. Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the headteacher. The Headteacher is the only member of staff permitted to post on the school's Facebook page.

Published content on the school website:

5.28. The headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

5.29. Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

5.30. Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.

5.31. Pupils are not permitted to take or publish photos of others without permission from the individual.

5.32. Any member of staff that is representing the school online, e.g. through blogging, must not disclose any confidential information regarding the school, or any information that may affect its reputation.

Mobile devices and hand-held computers:

5.33. The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

5.34. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

5.35. On no account may staff or pupils send inappropriate messages or images.

5.36. Photographs and videos of pupils or staff must not be published on social media sites.

5.37. No mobile device or hand-held computer owned by the school will be used to access public Wi-Fi networks.

5.38. The computing coordinator will review and authorise any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission from an ICT technician or the computing coordinator.

5.39. Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Network security:

5.40. Network profiles for each pupil and staff member are created, in which the individual must enter a username and personal password, where appropriate, when accessing the ICT systems within the school.

5.41. The ICT technician will ensure all school-owned laptops and computers have their encryption settings turned on, where possible.

5.42. Important folders, e.g. those including pupils' medical records, will be stored on Office365 and only accessed by authorised personal.

Virus management:

5.43. Technical security features, such as virus software, are kept up-to-date and managed by the ICT technician.

5.44. The ICT technician will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.45. Firewalls will be switched on at all times – ICT technicians will review these on a regular basis to ensure they are running correctly and to carryout any required updates.

5.46. Staff members will report all malware and virus attacks to the ICT technician immediately.

6. Cyber bullying

6.1. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online.

6.2. The school recognises that both staff and pupils may experience cyber bullying and will commit to using all reasonable strategies to prevent any instances occurring.

6.3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

6.4. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within Personal, Social and Health Education as well as Relationship, Sex and Health Education lessons.

6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

6.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

6.7. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

7. Reporting misuse

7.1. Wicklewood Primary School and Nursery will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreements, ensuring all pupils and staff members are aware of what behaviour is expected of them.

7.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to online safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

7.3. Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.

7.4. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher, if appropriate.

7.5. Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.

7.6. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding Policy, including Child Protection Policy.

Misuse by staff:

7.7. Any misuse of the internet by a member of staff should be immediately reported to the headteacher.

7.8. The headteacher will deal with such incidents in accordance with the school procedures and may decide to take disciplinary action against the member of staff.

7.9. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff. However, if suspected misuse by staff, then staff are to refer to Whistleblowing policy.

Use of illegal material:

7.10. In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.

7.11. Incidents will be immediately reported and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

7.12. If a child protection incident is suspected, the school's safeguarding procedure will be followed – the DSL / headteacher will be informed and the police contacted.