# CHEETWOOD COMMUNITY PRIMARY SCHOOL

# E-SAFETY POLICY

**Approved by the Governing Body**

**Signed**
**Chair of Governors**
**17/03/2021**

**To be reviewed Spring Term 2022**

**Judged to be GOOD by Ofsted in March 2018.**

***"This is a highly inclusive school, where everyone feels safe, respected and valued. Pupils enjoy school and are very keen to learn".***

learn together
grow together

## 1 INTRODUCTION

1.1 The DfE guidance Keeping Children Safe in Education 2020 has been used to inform this policy

1.2 This policy has been developed to ensure that all adults in Cheetwood Primary School are working together to safeguard and promote the welfare of children and young people.
**This policy has been ratified by the Governing Body at the meeting on 17 March 2021 and will be reviewed annually thereafter.**

1.3 E-Safety is a safeguarding issue, not an ICT issue, and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.4 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.5 The Headteacher or, in her absence, the Deputy Headteacher has the ultimate responsibility for safeguarding and promoting the welfare of pupils in the care of the school.

1.6 This policy complements and supports other relevant school and Local Authority policies.

1.7 The purpose of Internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the school's management information and business administration systems.

1.8 The Internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide pupils with quality access as part of their learning experience.

1.9 A risk assessment will be carried out before pupils are allowed to use new technology in schools and settings.

## 2 ETHOS

2.1 It is the duty of the school to ensure that every pupil in its care is safe. These safeguarding principles apply equally to the 'virtual' or digital world and have become much more pertinent recently as a result of the 2020-2021 COVID pandemic and the increase on remote learning for pupils. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

2.3 All staff have a responsibility to support e-safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour Policies.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

2.7 Staff, pupils, parents and carers will be proactively engaged in the implementation of e-safety principles.

2.8 E-safety principles will be embedded to ensure an effective and consistent approach when managing and dealing with e-safety issues that may arise.

E-safety principles will focus on the development of pupils' knowledge and understanding of the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Online behaviour
- How to identify online risks
- When and how to seek support

## 3 ROLES AND RESPONSIBILITIES

3.1 The Headteacher of Cheetwood Community Primary School will ensure that:

- All staff should be included in e-safety training. Staff must also understand that misuse of the Internet may lead to disciplinary action and possible dismissal.
- A Designated Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the school's Designated Persons for Safeguarding. The Designated Member of staff for E-Learning/Safety is Lee Hardy, who is also the school's ICT Leader.
- All temporary staff and volunteers are made aware of the school's e-learning/safety Policy and arrangements.
- A commitment to e-safety is an integral part of the safer recruitment and selection process of staff and volunteers.

3.2. The Governing Body of the school will ensure that:

- There is designated member of staff to take the lead on E-Learning/Safety within the school.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.

3.3 The Designated Member of Staff for E-Learning/Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the school's Designated Persons for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on e-safety.
- Ensure that all staff and volunteers have received a copy of the school's ICT Acceptable Use policy document.
- Ensure that all staff and volunteers understand and are aware of the school's E-Learning/Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network.

## 4 TEACHING and LEARNING

### Benefits of Internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to worldwide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students worldwide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The Internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DfE.

4.4 The Internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The Internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the pupils.

4.7 Pupils at the school will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Pupils at the school will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Pupils will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

4.10 The DfE Teaching Online Safety in School document (June 2019) will provide guidance for the teaching and learning of harms and risks associated with online behaviour (see Appendix A for harms and risks).

## 5 MANAGING INTERNET ACCESS

5.1 Developing good practice in Internet use as a tool for teaching and learning is essential. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.

5.2 Pupils will be taught what Internet use is acceptable and what is not and be given clear objectives for Internet use. Staff will guide pupils in online activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

5.4 If staff or pupils discover unsuitable sites, the URL and content must be reported to the Internet Service Provider via the ICT Leader.

5.5 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

## 6 MANAGING SCHOOL E-MAIL

6.1 Personal e-mail or messaging between staff and pupils should not take place.

6.2 Staff must use the school e-mail address if they need to communicate with pupils about their school work.

6.3 Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole class or group e-mail addresses are used throughout the school. Individual pupil emails may be used as part of teaching about responsible Internet use. The individual email accounts will then be deleted after the topic is completed.

6.4 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.5 Access in school to external personal e-mail accounts may be blocked.

6.6 Excessive social e-mail use can interfere with learning and will be restricted.

6.7 Pupils' e-mails will be authorised before sending to an external organisation.

6.8 The forwarding of chain letters is not permitted.

6.9 Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

## 7 MANAGING THE SCHOOL'S WEBSITE CONTENT

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used without the written consent of the pupils' parents/carers.

7.3 The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

7.4 The Headteacher will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected so that any pupils cannot be identified or their image misused.

7.7 Only the first names of pupils will be used on the website; pupils will only be named in group photographs so that they cannot be identified

7.8 Work will only be used on the website with the permission of the pupil and their parents/carers.

7.9 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.10 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

7.11 Staff members who need content uploading to the school website are responsible for checking the content that is being uploaded and passing to the Headteacher for final approval.

## 8 SOCIAL NETWORKING AND CHAT ROOMS AT SCHOOL

8.1 The school will control access to moderated social networking sites and educate pupils in their safe use.

8.2 Access to social networking sites such as Facebook, Twitter and Snapchat will be blocked through the school internet filter.

8.3 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.

8.4 Pupils will not be allowed to access public or unregulated chat rooms.

8.5 Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

8.6 Newsgroups will be blocked unless an educational need can be demonstrated.

8.7 Pupils will be advised to use nick names and avatars when using social networking sites.

8.8 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

8.9 Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of the Headteacher should always be sought first and language should always be appropriate and professional.

8.10 Any reports of bullying via social networking will be dealt with in accordance with the school's anti-bullying policy. This includes incidents of bullying that occur out of school hours.

8.11 Any pupil who abuses a member of staff on social networking sites will be disciplined in accordance with the school's behaviour policy.

8.12 Improper use of social media by a member of staff could amount to gross misconduct even if carried out via personal social media in the member of staff's own time. Staff will not discuss or comment upon school business on social networking sites. Any staff who make reference to specific school business will face disciplinary action. Misuse can qualify as grounds for dismissal.

## 9 MOBILE PHONES

9.1 Mobile phones or smart watches will not be used during lessons or formal times in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt in accordance with the school's behaviour and/or anti-bullying policies.

9.2 Use of cameras in mobile phones, smart watches or personal tablet technology by pupils will not be allowed; should special circumstances arise where it is felt that the use of mobile phone cameras is necessary, the agreement of the Headteacher should always be sought first, along with the permission of the relevant parents/carers.

9.3 Incidents of any pupil sending abusive text messages or making nuisance calls using mobile phones will be dealt in accordance with the school's behaviour and/or anti-bullying policies.

## 10 FILTERING

10.1 The school will work in partnership with parents/carers, the Local Authority, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 If staff or pupils discover unsuitable sites, the URL and content must be reported to the ICT Leader/E-Safety Co-ordinator, who will ensure the website is blocked and no longer accessible on the school network.

10.3 Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).

10.4 Regular checks by senior staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

10.6 Should staff require access to a blocked website, if it is deemed appropriate by the headteacher, a request for it to be unblocked can be made of the ICT Leader.

## 11 AUTHORISING INTERNET ACCESS

11.1 All staff must read and sign the school's ICT Acceptable Use policy before using any school ICT resources. Other adults not directly employed by the school (eg students on placement, supply staff, volunteer workers, parents/community users) will also be made aware of the school's policy on the acceptable use of ICT and asked to sign a statement of understanding before being allowed Internet access from the school site.

11.2 The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

11.3 The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied Internet or e-mail access.

11.4 On the admission of a new pupil into school, their parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'Acceptable Use' document and give permission for their child to access ICT resources.

11.5 Staff will supervise access to the Internet from the school site for all pupils.

## 12 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

12.1 When not in use, all video conferencing cameras will be switched off.

12.2 It is not appropriate to use photographic or video technology in changing rooms or toilets.

12.3 Staff may use photographic or video technology to capture and support school trips and appropriate curriculum activities.

12.4 Audio and video files may not be downloaded without the prior permission of the network manager.

12.5 Pupils must have permission from a member of staff before making or answering a videoconference call or making a video or audio recording in school or on educational activities.

12.6 Videoconferencing and webcam use will be appropriately supervised for the pupil's age.

12.7 Parents are not permitted to take photographs or video any school performances or assemblies unless in exceptional circumstances and only with express permission from the Headteacher

## 13 ASSESSING RISKS

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

13.5 The Headteacher will ensure that this E-Safety Policy is implemented and compliance with the policy is monitored.

13.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

## 14 INTRODUCING THE POLICY TO PUPILS

14.1 Rules for Internet access will be posted in all rooms where computers are used.

14.2 Responsible Internet use, covering both school and home use, will be included in the curriculum.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.

14.4 Pupils will be informed that Internet use will be closely monitored and that misuse will be dealt with appropriately.

## 15 CONSULTING STAFF

15.1 It is essential that teachers and learning support staff are confident about using the Internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's ICT Acceptable Use policy and will be provided with a copy of this policy and it's importance explained.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the Internet will be provided as required.
- Staff will be aware that Internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise members of staff who operate the monitoring procedures.

## 16 MAINTAINING ICT SECURITY

16.1 Personal data sent over the network will be encrypted or otherwise secured.

16.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

16.3 The ICT Technician commissioned by the school will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

## 17 DEALING WITH COMPLAINTS

17.1 Staff, pupils and parents/carers must know how and where to report incidents. Concerns related to safeguarding issues will be dealt with through the school's Safeguarding Policy and Procedures.

17.2 The school's Designated Person for E-Safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the Internet must be reported to the Headteacher immediately.

17.3 Pupils and parents/cares will be informed of the complaints procedure.

17.4 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

17.5 There may be occasions when the school must contact the police due to a serious breach of the school's behaviour policy. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of Internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework.
- Referral to the police.

## 18 PARENTS/CARERS SUPPORT

18.1 Parents/carers will be informed of the school's E-safety and ICT Acceptable Use Policies which may be accessed on the school website.

18.2 Any issues concerning the Internet will be handled sensitively to inform parents/carers without undue alarm.

18.3 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.

18.4 Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

18.5 A partnership approach will be encouraged with parents/carers and this will include practical sessions as well as suggestions for safe Internet use at home.

18.6 On the E-Safety page of the school website, there are a variety of monthly newsletters for parents to access. These newsletters cover a range of current e-safety topics and can provide parents with valuable information and support with e-safety matters.

## 19 REMOTE LEARNING: GOOGLE CLASSROOM

Google classroom is an online platform which the school uses to set remote learning due to self-isolation. For roles and responsibilities of teacher, pupils and parents, please refer to the Google Classroom User Agreement, found on the school website, along with the Remote Education Information for Parents, also on the website.

## 20 COVID-19

Since this policy was last reviewed in spring 2020, a coronavirus pandemic has swept across the world and affected all aspects of life, including that of education.

The school already has in place policies and procedures to provide and maintain safe and healthy working conditions, equipment and systems of work for all employees and pupils in relation to e-safety.

However, as a result of pupils needing to move to remote learning for short or extended periods and therefore spend more time online on a device, it has been necessary to develop new policies and procedures in order to protect health, safety and welfare even further.

Such measures have included

- Remote education provision information for parents, published on the school website, explicitly outlines expectations of the appropriate use Google Classroom of pupils
- Clear communication protocol in place for staff, parents/carers and pupils, published on the school website, explicitly outlines expectations when communicating online/electronically
- Only using a parent's/adult's email address to communicate school business with pupils
- Close and regular monitoring by staff of pupil online activity whilst using Google Classroom
- Staff following up as a matter of urgency with parents if their child's online activity whilst learning remotely on Google Classroom gives cause for concern
- Logging all e-safety concerns and action taken on CPOMS (the school's electronic recording system) so that it can be monitored by the E-Safety Leader and DSLs and further action taken if necessary
- Weekly safeguarding meetings where e-safety concerns can be discussed further by DSLs

## Appendix A

The following harms and risks are included in the DfE Teaching Online Safety in School document (June 2019). Staff will refer to this document when seeking guidance on how to approach teaching pupils about such harms and risks:

- How to navigate the internet and manage information.
- Age restrictions
- Content: how it can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Fraud (online)
- Password phishing
- Personal data
- Persuasive design
- Privacy settings
- Target of online content – including social media and search engines
- Abuse (online)
- Challenges
- Content which incites
- Fake profiles
- Grooming
- Live streaming
- Pornography
- Unsafe communication
- Impact of confidence
- Impact of quality of life, physical and mental health and relationships
- Online vs offline behaviours
- Reputational damage
- Suicide, self-harm and eating disorders.