



Chapelford Village Primary School

eSafety Policy

Learn
Achieve
Respect

Chapelford Village Primary School
Santa Rosa Boulevard
Warrington
WA5 3AL

Telephone: 01925 712554
Email: chapelford_admin@warrington.gov.uk

This policy is linked to:

- Anti-Bullying Policy
- Behaviour Policy
- Preventing Extremism & Radicalisation
- Safeguarding Policy

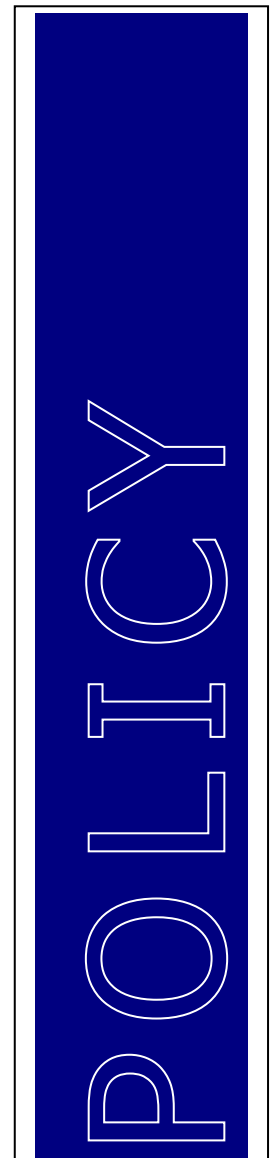
DOCUMENT STATUS

Version	Date	Action
1	February 2016	draft document
1	March 2016	Adopted by Governing Body

Ratified by governors on 17.3.16

Chair of Governors

Head Teacher



New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet is now regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe internet use by pupils in school and also while online beyond the classroom environment.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this eSafety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

1: Teaching and learning

1.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning across the curriculum.

1.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught how to evaluate Internet content
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2: Managing Internet Use

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor the LA can accept liability for the material accessed or any consequences of internet access. The use of school computer systems without permission or for inappropriate purpose could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly. The Headteacher, Governors and Computing Subject Lead will ensure that this policy is implemented and compliance with the policy is monitored.

2.1 Filtering

- The schools will work in partnership with parents, the LA and ABTEC to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable or illegal sites, the URL and content must be reported to the Computing Subject Lead. Parents of the children involved will be notified immediately.
- The Computing Subject Lead will ensure that regular checks are made to ensure that filtering methods selected are appropriate, effective and reasonable.
- Specific lessons will be included within the Computing curriculum that teaches pupils about eSafety.

3: The School Website (& VLE)

- The point of contact on the website should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name. Pupils' full names will not be used on the school website.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

4: Handling eSafety Complaints

- The Computing Subject Lead will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school Child Protection Procedures.

See appendix 1 for the eSafety Incident Log

5: Sharing the policy

5.1 Sharing the policy with pupils

- Rules for internet access will be posted in all classrooms where computers are used.
- A taught lesson on responsible internet use and eSafety will be included in the curriculum covering both school and home use.

- Instruction on responsible and safe use should precede internet access.

If using the internet at home:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.

5.2 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.
- All parents will receive support, information as and when available.

5.3 Staff Training

It is essential that all staff receive eSafety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal eSafety training will be made available to staff. An audit of the eSafety training needs of all staff will be carried out regularly. It is expected that some staff will identify eSafety as a training need within the performance management process.
- All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies.
- The eSafety Coordinator will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA/WBC and others.
- This eSafety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.

- The eSafety Coordinator will provide advice/guidance/training as required to individuals as required.

6: Prevent

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering system at Chapelford Village Primary blocks inappropriate content, including extremist content. Where staff, pupils or visitors find unblocked extremist content, they must report it to a senior member of staff immediately. Young people may be vulnerable to a range of risks as they pass through adolescence. They may be exposed to new influences and potentially risky behaviours as they begin to explore ideas and issues around their identity.

There is no single driver to radicalisation, nor is there a single journey to becoming radicalised. The internet however, simply creates more opportunities to become radicalised, since it is a worldwide 24/7 medium that allows pupils to find and meet pupils who share and reinforce your opinions.

[See Prevent Extremism Policy for further details]

7: Data Protection

7.1 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.


7.2 The use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet. E.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes. However should circumstances require, images may be taken on staff owned equipment provided that at the first available opportunity they are transferred to the school's network / blog and deleted from the staff device.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Appendix 1: eSafety Incident Log

	eSafety Incident Log		
	Reported by:		Reported to:
	Date:		Date:
<p>Incident Description: <i>Describe what happened, involving which children and/or staff and what action was taken</i></p>			
Review Date:			
Result of Review:			
Signature of Subject Lead:			Date:
Signature of Headteacher:			Date: