Cogan Primary School
Ysgol Gynradd Cogan

Social Media Policy
Use of Mobile Phones and Digital Photography Policy

Cogan Primary School/Ysgol Gynradd Cogan

Social Media Policy - Use of Mobile Phones and Digital Photography Policy

Social media and social networking sites play an important role in the lives of many of our children. It is recognised that the use of social media bring risks, but equally there are many benefits. This document gives clarity to the way in which social media are to be used by pupils and school staff at Cogan Primary School.

Social Media sites such as 'Twitter' and 'Facebook' state that children should be 13 years of age to use them (this was initially developed from American law). Therefore, no primary age children should be using or accessing these types of social media sites.

There are five key aspects to the use of social media:
A. The use of social networking sites by pupils within school.
B. Use of social networking by staff in a personal capacity.
C. Creation of network accounts by staff for use in education.
D. Comments posted by parents/carers.
E. Dealing with incidents of online bullying.

A. The use of social networking sites by pupils within school.

The school's policies make it clear to staff, pupils, governors and parents what use of social media is allowed. This states that, **'Social network sites should never be accessed/used within school by pupils independently'**.

Notes:
If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate.
The school e-safety policy states sanctions for breaching the policy.

B. Use of social networking by staff in a personal capacity.

It is possible that a high proportion of staff will have their own social networking site accounts.
It is important for them **to protect their professional reputation** by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff regularly at staff meetings:

i. Staff must never add pupils as friends/associates into their personal accounts for example: Instagram, Twitter, Pinterest, Tumblr etc...
ii. Staff must not post pictures or comments of school events without the Headteacher's consent.
iii. Staff must not use social networking sites within lesson times.

iv. Staff can only use social networking in a way that does not conflict with the current National Teacher's Standards.
v. Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
vi. Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.

Inappropriate use by staff should be referred to the Headteacher in the first instance and then the LA Safeguarding Officer.

C. Creation of network accounts by staff for use in education.

All social media sites must be approved by the Headteacher in advance of any educational work being undertaken.

D. Comments posted by parents/carers.

Parents and carers will be made aware of their responsibilities via Hwb+ and monthly newsletters regarding their use of social networking. Methods of school communication regarding e-safety and safe use of social media will be posted in the prospectus, on the website, Hwb+, newsletters, letters and verbal discussion.

i. Parents are not expected to post pictures of pupils other than their own children on social networking sites and should respect other parents' rights regarding this.
ii. Parents should make complaints through official school channels rather than posting them on social networking sites.
iii. Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

E. Dealing with incidents of online bullying

The schools e-safety and/or Anti Bullying Policy makes sanctions regarding bullying using new technologies very clear.

'The Behaviour and Discipline Policy' indicates that the school can take action against incidents that happen outside school if it:

i. Could have repercussions for the orderly running of the school or
ii. Poses a threat to another pupil or member of the public or
iii. Could adversely affect the reputation of the school.

Use of social networking sites to harass, bully or intimidate is covered by law irrespective of when/where the post is made.

Safeguarding of Children

Use of Mobile Phones, Ipads/tablets and Digital Photography Policy

Children have their photographs taken to provide evidence of their achievements for their development records. **Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of school children for their own purposes during the school day.**

Procedures

i. Under the data protection act of 1998 school must seek parental consent to take photographs and use film recorders. Photographs will be stored on the school network and Hwb+ which is pass word protected, when photographs are no longer required, they will be shredded or deleted from the school network.

ii. Photographs can be printed in the setting by staff and images used appropriately.

iii. Photographs may be taken during indoor and outdoor play and learning and displayed in school and in albums or a child's development records for children and parent /carers, governors, Estyn, LA officers (on Hwb+ which is a password protected learning platform), to look through.

iv. Often photographs may contain other children in the background.

v. Events may be recorded by film recorders or photographs taken by staff and parent/carers, but always in full view of all attending. Parents must not post/upload photographs or film recorded on the school premises on any social media platforms e.g. Facebook, Twitter, Youtube, Instagram etc…

vi. On occasion the school might like to use photographs of children taking part in an activity to advertise/promote the school via the website etc…, however in this instance, parental permission will be required. (Home/School agreement signed on school entry and/or letters of consent as appropriate)

Use of photographs on the school Twitter site will be of hands, feet or the back of children completing activities, although some permitted images can be used appropriately.

vii. **Visitors may only use their phones in the foyer or outside the building and should be challenged if seen using a camera inappropriately or photographing children.**

viii. The use of cameras and mobile phones are prohibited in toilets and changing areas.

ix. Staff are asked not to make personal calls during their working hours. However in urgent cases a call may be made or accepted if deemed necessary and by arrangement with the Headteacher.

x. All school cameras and film recorders should be kept securely at all times and used with appropriate authority.

xi. No devices such as phones or Ipads/tablets should be brought in from home to use in school by pupils. This ensures that filters are used appropriately.

Policy date: February 2026 Agreed by the Governing Body
Reviewed - as necessary due to media changes

Appendix 1:

Letter sent to all schools December 2013 from the Vale of Glamorgan Council

Social Networking and your School

The School encourages the responsible use of the Internet and social media to support learning and communication with parents. Parents are increasingly using social networking websites and mobile “apps” such as Facebook, Twitter and Snap Chat to talk to their friends.

Many users believe that they are writing for a closed group of friends, unaware that the information they have posted may be publicly available and read by a much wider audience. Some parents may wish to openly discuss matters relating to school.

The Headteacher and governing body are fully committed to the continued improvement of our school. We welcome feedback from parents/carers and will always try to resolve any concerns as quickly as possible. A small number of parents at some schools have used social networking to make inappropriate comments about schools or individual teachers. Statements, defamatory or otherwise can have the same legal consequences as if they were made directly to another person and in some cases criminal offences can be considered under a number of Acts including but not limited to the Malicious Communications Act 1988, Communications Act 2003, Protection from Harassment Act 1997, Criminal Justice Act 2004 and Public Order Act 1986.

Consequences for criminal offences under the above legislation include cautions, fines and significant prison sentences.

The sort of communications that are capable of amounting to criminal offences include 1) credible threats of violence to person or damage to property, 2) communications which specifically target an individual and may constitute harassment or stalking and 3) communications which are grossly offensive, indecent, obscene, menacing or false.

If you have concerns about anything that happens in school please speak to your child’s class or form teacher or the Headteacher who will do their best to resolve the matter. If you are still unhappy, the school has a complaints procedure which will ensure your concerns are investigated thoroughly and appropriate action is taken.

Appendix 2: E-safety Policy

COGAN PRIMARY SCHOOL

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Vale of Glamorgan Community Network including the effective management of Websense filtering.
- National Education Network standards and specifications.

School e-safety policy

2.1 The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the Vale e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors and the PTA.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: Staff and Governors
- It was approved by the Governors on: 03/2015

2.2 Teaching and learning

2.2.1 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.

2.2.3 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

2.2.4 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.

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Vale county council.

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

2.3.5 Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

2.3.6 Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read and adhere to the school's 'Acceptable Use of the Internet Agreement'
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

2.4.2 Assessing risks

- 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 Vale county council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- 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.
- Pupils and parents will be informed of the complaints procedure.

2.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Hwb+ site/website.

Policy – Social Media

This is to confirm that the Governing Body of

Cogan Primary School
Ysgol Gynradd Cogan

has accepted the attached policy at the Governing Body meeting held on

February 2026

Signed: K John

Chair of Governing Body

Date: 04/02/26