Gomer Junior School

Online Safety Policy
2020

Aims

The aim of this policy to promote the safe use of the ICT. All ICT use should include teaching the children about safeguarding concerns, including combating radicalisation, and good practice for avoiding unsafe situations and practices for reporting any violations. The policy has been written after consulting "KCSIE", September 2019 and "The Prevent Strategy", June 2015.

Our Online Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The Designated Safeguarding Lead works closely with the Computing Leader
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually.

Teaching and learning

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 pupils with quality Internet access as part of the curriculum.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access is provided by Hampshire County Council and includes filtering appropriate to the age of pupils. An additional filtering set is available in school administration networks only and enables staff access to additional resources.
- 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

- We aim to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

<u>Managing Internet Access</u>

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the IT lead for the Gosport and Fareham Multi-academy Trust.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive 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.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- 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.

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 Head Teacher takes overall editorial responsibility.

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 including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained when pupils join our school, before photographs of pupils are published on the school Web site.

Social networking and personal publishing on the school learning platform

- The GFM block/filter access to social networking sites unless short-term access is required for a specific educational project.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform other than those authorised by the school e.g. Home Learning (Google Classroom)
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Managing filtering

- The school will work in partnership with Hampshire County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported ICT Services Help Desk by email it@helpdesk.gfmat.org

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, including calls originating within the learning platform.
- Videoconferencing will be appropriately supervised for the pupils' age.

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 except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden. Pupils must not access their mobile devices until off-site.

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

Policy Decisions

Authorising Internet access
- All staff must adhere to the Code of Conduct in relation to internet access and mobile technology usage.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- The wifi code can be shared with visitors.

Assessing risks
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling Online 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 Exec. Head or Associate Head Teacher.
- 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.
- Discussions will be held with the Police and or PCSO to establish procedures for handling potentially illegal issues.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety policy.

Communications Policy

Introducing the Online Safety policy to pupils

- Online Safety will be posted in the majority of networked areas.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will have regular Online Safety sessions where different aspects of online safety are explored and taught. These will be appropriate to the age of the pupil's and are adaptable as the internet age also adapts.
- As well as set Online Safety sessions, teachers will address any online safety concerns as and when, and online safety will be incorporated into ICT and Computing sessions

Staff and the Online Safety policy

- All staff will be given the School Online 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.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will act as clear role models when using the internet in front of pupils as part of a lesson and Online Safety will be discussed when this occurs.

Enlisting parents/carers support

- Parents' and carers attention will be drawn to the School Online Safety Policy in newsletters, website, home school agreement, the school prospectus.
- Parents and carers will from time to time be provided with additional information on Online Safety e.g. school Facebook posts and Online Safety workshops.