Grangefield School
Flying high. Spreading our wings.

Grangefield School E-Safety Policy

What is e-safety?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

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

Our school e-Safety Policy

The schools e-safety will be overseen by the Computing coordinator, Abi Stokes. It has been written using guidance from LEA advisors.
It has been agreed by the senior management team and approved by governors.
The e-Safety Policy will be reviewed annually.

Why is Internet Use Important?

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

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils world-wide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority and DfE; access to learning wherever and whenever convenient

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All children complete their own acceptable use agreement on entry to Grangefield and this is kept in a central store and covers them for their time at Grangefield. Parents will also be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the Computing coordinator or technician.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail and should only access their class email when supervised.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be filtered by SWGFL.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- E-mail should only be accessed through a web browser on any device that is being used. The use of the Outlook App is not permitted.
- The forwarding of chain letters is not permitted.

Social Networking

- Social networking sites and newsgroups have been blocked by SWGFL filtering systems
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the LEA and our internet service providers SWGFL, to filter inappropriate sites.

Video Conferencing

- 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.

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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

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 and admin staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will never be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers has been obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- No data or pupil information will be stored on Dropbox. This is to be used as a file sharing platform for teachers administration purposes.

Protecting Personal Data

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

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.
- The school should audit computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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.

Communication of Policy

Pupils

- Rules for Internet access will be posted in the ICT suite. (SEE BELOW)
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School e-Safety Policy and its importance will be explained.
- All staff will sign the Acceptable Use Agreement and this will be regularly updated (twice annually) to meet changes in technology and changes in personal circumstances.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in the school prospectus and on the school Web site.
- Parents will annually sign the consent form attached to this policy.

E-Safety Coordinator / Officer

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor – Mrs A Williams.

The role of the E-Safety Governor will include:
• regular meetings with the E-Safety Co-ordinator / Officer
• regular monitoring of e-safety incident logs
• regular monitoring of filtering / change control logs
• reporting to relevant Governors committee / meeting

To be reviewed May 2018

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

B. Stoneham & J. Barrett

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

e-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

Our School - e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed. These rules can be found on our website: http://grangefield.gloucs.sch.uk/welcome-to-grangefield-school/school-policies/ e-Safety Policy.

Publicity/Third Party Organisations
From time to time the school will be visited by members of the press and or other organisations such as trip venues/workshops, who may be allowed to take photographs of children ie sporting events, plays, charity events and awards etc. Those images may be used for promotional materials or could appear on those organisations websites. Please sign if your child is allowed to be included:

Signed:
Print Name:
Date:

Parent's Consent for Web Publication of Work and Photographs
I agree that my son/daughter's work may be electronically published on our website/blog. I also agree that appropriate images and video that include my son/daughter may be published on our website/blog subject to the school rule that photographs will not be accompanied by pupil names:

Signed:
Print Name:
Date:

Parent's Consent for Internet Access
I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:
Print Name:
Date:

Social Media
I have read the school Social Media Policy.

Signed:
Print Name:
Date: