Gretton Primary School

Internet and eSafety Policy

Contents

1. Rationale

At Gretton School we believe that the Internet is a vital source of enrichment and information for children. Online activities provide countless new opportunities for communication, expression and learning, and the Internet has become a fundamental part of modern life. Therefore, all children deserve to be well-versed in its use as these skills will be essential for daily life. We also recognise that unregulated and untrained use of the Internet represents a real risk to children due to the broad range of material that can be viewed and the anonymous nature of Internet use.

Gretton School recognises an obligation to maintain and promote the safe use of the Internet for its pupils and is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

2. Definitions

eSafety is the term used for all safety issues in relation to IT use, particularly but not exclusively online activity. Online activity can be any communication activity using electronic means, including the Internet, emails, mobile phone texting or messages via games consoles. Such activity can be in-school or outside of school. Gretton School considers that activity outside of school which will affect school life is bound by the contents of this Policy.

3. Aim

We seek to provide every child with a safe online environment in which to grow and learn so that they may maximise their ability to express themselves and seek information without risk of contact with unsuitable material. Furthermore, it means equipping children with the skills they need to make sensible and safe decisions when working online, to manage the risk of unwanted contact with people, images or information that is not appropriate for their age. Most importantly we aim to teach children to communicate responsibly.

4. Objectives

Our objectives are to:

- Provide a safe, robust networked internet access point which has a managed filter system to prevent access to unsuitable material.
- Foster sensible rules and behaviours to govern browsing and online activities so that children are equipped to govern themselves as they grow older.
- Provide resources and information to educate children and carers as to the available support for recognising online issues and reporting instances of unwarranted contact online.
- Create a set of procedures which enable the school staff to confidently use the online resources in school with children, and support them should any issue arise.

5. Strategies and procedures

5.1 Managing Internet Access

5.1.1 Information system security

School IT system security will be reviewed regularly in conjunction with SWGfL (curriculum) and local authority (SIMS/admin)

Virus protection will be installed and updated regularly.

5.1.2 E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

5.1.3 Published content and the school website

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

The Co-headteachers or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

5.1.4 Publishing pupils' images and work

Pupil photographs will be used only with permission for reasonable promotion of school events and celebration of achievements.

Photographs that include pupils will be selected carefully so that individual children cannot be identified by name or their image misused.

Pupils' full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Work can only be published with the permission of the pupil and parents/carers.

5.1.5 Social networking and personal publishing

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

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, their friends or their location.

Pupils should not place personal photos 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. Pupils should only invite friends known to them in 'real life' and deny access to others.

5.1.6 Managing filtering

The school will work in partnership with Gloucestershire LA and the Internet Service Provider (currently SWGfL) to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the Co-headteachers.
The Senior Leadership Team will implement checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

5.1.7 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.

5.1.8 Managing emerging technologies

Emerging technologies / personal devices (eg. iPads) will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Members of staff are aware and vigilant to the fact that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used by pupils in school. In exceptional circumstances, if a parent wishes their child to have access to a mobile phone for before or after school use, this request should be in writing and the device will be retained in the school office during the school day.

Games machines including the Sony Playstation, Microsoft Xbox, Nintendo DS and others have Internet access which may not include filtering. Therefore, these devices will not be allowed in school.

Staff will use the school phone where contact with pupils is required.

5.1.9 Protecting personal data

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

5.2 Policy Decisions

5.2.1 Authorising Internet access

All staff must read and sign the Acceptable Use Policy (AUP) agreement (Appendix A) and this policy before using any school IT resource.

The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

Parents/carers will be asked to sign and return an Acceptable Use Agreement (Appendix B) consent form which will accompany information sent home regarding Safe Use of the Internet.

5.2.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor SWGfL can accept liability for any material accessed, or any consequences of Internet access.

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

5.2.3 Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff and an incident log kept. The school does not tolerate cyber-bullying and will follow the procedures within the anti-bullying policy when dealing with any incidents.

Any complaint about staff misuse must be referred to the Co-headteachers.

Complaints of a child protection nature will be dealt with in accordance with school Safeguarding / child protection procedures. Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

5.2.4 Community use of the Internet

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

5.3 Communicating e-Safety

5.3.1 Introducing the e-safety policy to pupils

e-Safety rules will be posted in all rooms where computers/laptops/iPads are used.

Pupils will be informed that network and Internet use will be monitored.

A programme of training in e-Safety has been developed, based on materials appropriate for the primary age-range.

5.3.2 Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.
Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor IT use will be supervised by the co-headteachers and work to clear procedures for reporting issues.

Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

5.3.3 Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.

The school will maintain a list of e-safety resources for parents/carers. This will accompany the Safe Use Agreement.

6. Roles

6.1 Governors

Governors will oversee the implementation of this policy and the associated Safe Use Agreement document. The Governors Curriculum group will consider the implications of eSafety in the teaching of IT/Computing. A Safeguarding Governor is also appointed to oversee eSafety as a separate school issue.

6.2 Co-headteachers

The Co-headteachers will ensure that all staff are aware of and comply with the school's policy for Internet use and eSafety. It will be the Heads' responsibility to deal with any issues of online abuse affecting school that may occur.

6.3 IT Technician

The IT technician is responsible for the technical aspects of the school's e-safety and security systems through maintaining links and communication with the provider SWGfL. The technician sets up usernames, logins and passwords to enable staff and pupils to use the IT systems securely.

6.4 Staff

All staff will be aware of and comply with the guidelines of this policy and the Acceptable Use Policy agreement. Senior teachers and the IT coordinator will lead the development of eSafety processes but staff will have a shared responsibility to monitor and assess online activity within their classes. Staff will provide guidance and teaching to pupils and report any issues to the Co-headteachers.

6.5 Parents

Parents will be aware of and be asked to sign the Safe Use Agreement. Parents will be provided with suggestions of materials to support them in being responsible for monitoring and assessing children's online activity outside of school.

6.6 Pupils

Pupils will be responsible for their own safety and that of their peers by following the guidance of the Safe Use Agreement (Appendix C) and being mindful of the issues that using the Internet generate. They will also report any suspicious or unwanted online material or contact to a trusted adult immediately upon encountering it.

7. Review period and next review date

Last review: Summer 2015 Next review: Summer 2016

8. Guidance on teaching

An e-safety education programme has been established across the school, with sessions being delivered each term.

FS & KS1 will use units from 'Hector's World':

Details, Details
Welcome to the Carnival
It's a Serious Game
The Info Gang
Heroes
You're Not Alone

KS2 will use the 'Smart Rules':

Smart crew
What should I accept?
What is reliable?
What should you keep safe?
Who should you tell?
Be careful when meeting up

8.1 Why the Internet and digital communications are 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 high-quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

8.2 Internet use will enhance and extend learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

8.3 Pupils will be taught how to evaluate Internet content

The school will ensure that staff and pupils are aware that the use of Internet derived materials should comply with copyright law.
Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

9. Links

The e-Safety Policy relates to other policies including those for IT/Computing, Safeguarding and Anti-bullying.

(See appendix A, B & C below)

Appendix A

Gretton Primary School

Staff (& Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of all members of the school community, both within school and in their lives outside. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy (AUP) is intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
• that staff are protected from potential risk in their use of IT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to IT to enhance their work, to enhance opportunities for pupil's learning and will, in return, expect staff and volunteers to agree to be responsible users.
This AUP links with the school's Child Protection/Safeguarding Policies.

Acceptable Use Policy Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of ICT/Computing for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT/Computing. I will, where possible, educate the young people in my care in the safe use of IT and embed e-safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the IT systems, email and other digital communications.
• I understand that the rules set out in this agreement also apply to use of school IT systems (eg laptops, email, iPads etc) out of school.
• I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal use within the policies and rules set down by the school.
• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
• I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school IT systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the school website) it will not be possible to identify by full name, or other personal information, those who are featured.
• I will only use networking sites in school in accordance with the school's policies.

• I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
REMEMBER: There are risks attached to using personal email addresses / mobile phones / social networking sites for communications with pupils and parents/carers.
• I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
• When I use my personal hand held / external devices (PDAs / laptops / mobile phones / iPads / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
During the school day, I will ensure that my mobile phone is on silent and out of sight when I am working, and I will only check or use it during an 'off-duty' break or lunchtime.
• I will not use personal email addresses on the school IT systems.
• I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
• I will ensure that my data is regularly backed up, in accordance with relevant school policies.
• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies and the IT Technician or Co-ordinator has been consulted first.
• I will not disable or cause any damage to school equipment, or the equipment belonging to others.
I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted.
• I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:
• I will ensure that I have permission to use the original work of others in my own work.
• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
• I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

STAFF/ VOLUNTEER ACCEPTABLE USE POLICY AGREEMENT

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: _____

Signed: _____

Date: _____

STAFF/ VOLUNTEER ACCEPTABLE USE POLICY AGREEMENT

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: _____

Signed: _____

Date: _____

Appendix B

Gretton Primary School
Parent / Carer Acceptable Use Policy Agreement

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 and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and raise awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.
This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour

The school will try to ensure that pupils will have good access to ICT/Computing to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Parents are requested to sign the 'Permission Form' below to show their support of the school in this important aspect of education.

Permission Form

Parent / Carers Name | Pupil's Name

- As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to IT systems at school.
- I understand that my son / daughter will receive e-safety education to help them understand the importance of safe use of ICT, both in and out of school, and that s/he will be asked to follow a set of simple rules (attached).
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed | Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate the huge number of successes we have in our school through their publication in newsletters, on the school website and occasionally in the public media. The school wishes to comply with the Data Protection Act by seeking permission from parents/carers before taking images of any member of the school. **For this reason we request that if you have any reservations regarding this matter, and/or you do not wish images to be taken and used as stated above, that you write and let the school know as soon as possible for the new school year, but by the second week in September at the latest.**

Appendix C

Pupil Acceptable Use Agreement
E-Safety Rules for Key Stage 2

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Pupil Acceptable Use Agreement

E-Safety Rules for KS1 & Reception

- I must only use the computers when a grown up is with me.

- **I m**ust not put my name or where I live on the Internet.

- I must not put my friend's names or where they live on the Internet.

- I must tell a grown up if I see something that scares me on the Internet

Gretton Primary School

Pupil Acceptable Use Agreement Form
KS2

Once you have read and understood the Pupil Acceptable Use Agreement / eSafety Rules please complete the sections below to show that you agree to follow them. If you do not sign and return this agreement, access will not be granted to school IT systems.

I have read and understood the e-Safety Rules and agree to follow them in order to support the safe use of ICT/Computing at Gretton School.
I understand that I am responsible for my actions when using IT and that if I do not follow the rules I may lose access to any IT systems when in school.

Name of Pupil:_____**Class:** _____

Signed: _____ **(Child)**

Gretton Primary School

Pupil Acceptable Use Agreement Form
KS1/Reception

Once you have read and discussed the eSafety Rules with your child, please complete the sections below. If you do not sign and return this agreement, access will not be granted to school IT systems.

We have discussed the e-Safety Rules and my child agrees to follow them in order to support the safe use of IT/Computing at Gretton School.

Name of Pupil:_____**Class:** _____

Signed: _____