Gladstone Primary School

E-Safety Policy.

This Policy applies to all staff and pupils from EYFS to Year 6 (including the Nurture Provision)

Policy Update: 2012
Policy Update: March 2016
Chair of Governors: Mrs Christine Bartley
Headteacher: Mrs Elaine Preston

E-Safety includes Internet technologies and electronic communications such as mobile phones and other internet enabled devices eg Xbox, Wii, iPad's and games consoles 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 Behaviour, Bullying, and Child Protection.

The C&YP Core E-Safety Policy

This core E-safety Policy provides the essential minimal school e-safety policy and has been approved by the Children and Young People's Services.

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 including the effective management of Websense filtering.
- National Education Network standards and specifications.

Further Information

E-Safety information is available from Stoke-on-Trent Safeguarding Board web site:
http://www.safeguardingchildren.stoke.gov.uk/ccm/content/safeguarding-children/professionals-folder/child-safety/e-safety.en

Writing and reviewing the E-safety policy

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 has a designated E-Safety Leader – Mrs Preston. The Designated Child Protection Leader, the Headteacher, also plays an important role in decision making regarding safeguarding and is made aware of all issues.

Our e-Safety Policy has been written by the school, building on the Stoke-on-Trent E-Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by governors and the E-Safety Committee.

The E-Safety Policy and its implementation will be reviewed annually. The E-Safety Policy was adopted by the Governing Body.

Teaching and Learning

New Technologies and Internet use 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 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.

- 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 will be given clear objectives for Internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of effective knowledge location, retrieval and evaluation.

Pupils will be Taught how to Evaluate Internet content.

- The school will ensure that the copying and subsequent 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.

Pupils will be Taught How to Stay E-safe.

- Curriculum planning will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as e-mail, mobile phones and social networking sites.
- E-safety delivery will be mapped across the curriculum to ensure full coverage.
- E-safety delivery will include the safe use of mobile phones and other internet enabled device, e.g., x box, I pad, Wii, etc.

Managing Internet Access

Virus protection will be updated regularly on all networked computers.
School ICT systems capacity and security will be reviewed regularly.

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.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Public Web Published Content and the School Web Site.

- The contact details on the website 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.
- The website complies with the school's guidelines for publications, including respect for intellectual property rights and copyright.

Web Publishing Pupils' Images and Work

- Images, published to the web, 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 website, particularly in association with photographs.
- Written permission from parents/carers will be obtained before images of pupils are published electronically
- Pupil's work can only be published to the website with the permission of the pupil and parents/carers.

Social Networking and Personal Publishing

- Newsgroups will be blocked unless a specific use is approved.
- Access to Social Networking Sites is not permitted in school.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents/carers will be advised that the use of social network spaces, outside school based controlled systems is inappropriate for primary aged pupils, unless strictly supervised.
- Staff and pupils should be advised not to publish specific and detailed private thoughts on Social Networking Sites.

Managing Filtering.

- The school will work with Becta and the WAN Managed Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, the URL must be reported to Mr Preston (IT Technician), Mrs Preston and Mrs Swift or the WAN Managed Service Provider helpdesk.

Managing Remote Teaching/video-Conferencing.
The Equipment and Network.

- Full IP videoconferencing will use the national educational or the schools' broadband network to ensure quality of service and security.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- School videoconferencing equipment will not be taken off school premises without permission, since use over a non-educational network (e.g. the internet) cannot be monitored or controlled.

Users.

- Pupils will ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age.
- Parents/Carers will agree for their children to take part in videoconferences, probably in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Only key administrators will be given access to the videoconferencing system, web or other remote control page available on larger systems.

Content.

- When recording a videoconference lesson, written permission will be sought by all sites and participants. The reason for the recording is given and the recording of videoconference is clear to all parties at the start of the conference.
- Recorded material will be stored securely.
- If third-party materials are to be included, recordings will be checked that they are acceptable to avoid infringing the third party intellectual property rights.
- Dialogue will be established with other conference participants before taking part in a videoconference. If it is a non school site it is checked that they are delivering material that is appropriate for the class.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden.

Protecting Personal Data and Passwords

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All pupils are allocated an individual username and password with which to access the computers, their e-mail accounts.
- Key Stage 1 and 2 pupils are told their personal usernames and passwords and encouraged to ensure these remain secret.
- Passwords are changed if necessary to maintain security.

Relevant staff (I.e. class teachers) have access to relevant pupil passwords.

Policy Decisions

Authorising Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes 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.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- At Key Stage 1 access to the Internet will be by adult demonstration or by directly supervised access to specific, approved on-line materials.
- Parents/Carers will be asked to sign and return a consent form.
- Mr Preston (IT Technician) will monitor computer and internet use on a weekly basis. Any concerns will be reported to Mrs Preston (Headteacher). Issues will be dealt in the appropriate way with and evidence recorded.

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 Stoke-on-Trent City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit IT provision to establish if the E-safety Policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff. The Headteacher must be informed.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with our Child Protection Procedures.
- Pupils and parents/carers will be informed of the complaints procedure.
- Parents/Carers and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy will include:
  - interview/counselling by the head of key stage;
  - informing parents/carers or carers;
  - removal or restriction of Internet or computer access for a period.

Community use of the Internet

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

Cyberbullying – Understanding and Addressing the Issues

- While cyberbullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or MSN, are becoming more frequent.
- As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.
- As felt appropriate for the age and use of technology by the pupils:
- The school's Anti-Bullying Policy and/or school behaviour policy will address cyberbullying. Cyberbullying will also be addressed in IT, PHSE and other relevant lessons and is brought to life through activities. As with other whole-school policies, all staff and young people will be included and empowered to take part in the process.
- Pupils, parents/carers, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents/carers will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse via the school Bullying Policy and the school Behaviour Policy.
- Parents/Carers will be provided with an opportunity to find out more about cyberbullying through: session for parents/carers, guidance, websites published in newsletter and on the school website. Courses for parents are also available.

Cyberbullying - How will risks be Assessed?

- The school will take all reasonable precautions to ensure against cyberbullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.
- The school will proactively engage with KS2 pupils in preventing cyberbullying by:
    - understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages;
    - keeping existing policies and practices up-to-date with new technologies;
    - ensuring easy and comfortable procedures for reporting;
    - promoting the positive use of technology;
    - evaluating the impact of prevention activities.
    - Records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities.

How Will Cyberbullying Reports/Issues be Handled?

- Complaints of cyberbullying will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher.
- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.
- Pupils and parents/carers will be informed of the complaints procedure.
- Parents/Carers and pupils will need to work in partnership with staff to resolve issues.

Communications Policy

Introducing the E-safety Policy to Pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year and as the need arises.
- Pupils will be informed that network and Internet use will be monitored.
- E-Safety lessons through the IT curriculum and targeted focus days raise the awareness and importance of safe and responsible internet use/use of mobile phones.
- Instruction in responsible and safe use should precede Internet access.

- An E-Safety module is included in the ICT programmes covering both school and home use.
- Children are **not** allowed to bring in their own equipment from home to access to the internet.
- Teacher must speak regularly to the children about internet safety and ensure that they understand the rules.
- Internet safety is also reinforced in school assemblies.

Staff and the E-Safety Policy

- All staff will be given the School E-Safety Policy and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues. This monitoring will also be checked by a Member of the Governing Body as part of regular safeguarding checks.
- Staff must view all on-line content before showing them to the children eg, video clips from utube.
- Classrooms must display E-safety rules which have been devised by the children.

Enlisting Parents/Carers Support

- Parents/Carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure, on the school website and through parents/carers awareness sessions held regularly.
- Parents/Carers views and ideas will be canvassed by questionnaires.
- Parents/Carers are welcome to bring any issues to staff to deal with.
- Parents/Carers will be kept informed about e-safety teaching as is takes place each term.

Unsuitable Material

Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.
The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Administrator
3. Logging the incident
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future.
5. Parents will be informed.

This Policy should be read in Conjunction with our Social Networking Policy and Safeguarding Policy.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	**Key E-Safety issues**	**Relevant Websites**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Networked favourites Ikeepbookmarks.com SCORE minisites
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search - Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	School Net Global E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites for feedback.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils should be encouraged to report any inappropriate comments.	SCORE Showcase Making the News Podcasts
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within blogs, chat rooms or online forums.	Only blogs/chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype FlashMeeting VLE
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum

E-Safety Audit – Primary / Special

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an e-Safety Policy that complies with C&YP guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents/carers at:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for staff?	Y/N
Has e-safety training been coherently planned and delivered for pupils?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the school e-Safety Rules?	Y/N
Have school e-Safety Rules been set with pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access (e.g. Stoke-on-Trent Educational WAN).	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Has the school filtering policy been approved by SMT? (N/A unless school has taken over responsibility)	Y/N
If the school has taken responsibility for its own webfiltering, have appropriate members of staff attended training on the filtering system and are appropriate procedures in place?	Y/N
Is an ICT security audit advisable (possibly using external expertise) to ensure e-safe practice technically and educationally?	Y/N