This policy has been developed to follow the guidelines set by the Gloucester Safeguarding Children Board and has been ratified by Governors. It covers use of digital media by staff and pupils.
This policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Child Protection.

Online-Safety is a key area of safeguarding and is the responsibility of all staff.

Online -Safety encompasses all digital technologies, the Internet and electronic communications such as mobile phones, as well as digital 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.

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.
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.
At Harewood Junior School we understand the responsibility to educate our pupils on Online -Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

End to end Online -safety

Online -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 Online-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from a certified Internet service provider (ISP) such as South West Grid for Learning (SWGfL).
- National Education Network standards and specifications.

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 guidance for Internet use both in and outside of school
- 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

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.

Safeguarding

The internet offers children access to a wide range of resources. However, it also poses a significant risk to safeguarding. All staff must ensure that they understand the risks faced by children in the modern digital age. Staff must report any concerns regarding digital safeguarding to the school's safeguarding lead. This includes any disclosures of potential safeguarding risks which have occurred inside or outside of school. This may include, but is not limited to, abuse via social media, emails, text messages, instant messaging etc., exposure to pornography or explicit images, potential grooming, playing games or watching videos below the legal age limit, buying age restricted items online, hacking and data violations.

Managing Internet Access

All access to the internet at school is through our certified ISP, SWGfL, which provides firewalls and filtered protection to all internet connections. The service's filtering options can be found at (http://www.swgfl.org.uk/Services/SWGfL-Filtering).

Information system security**,** school ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly by the ICT technician.

Security strategies will be discussed with SWGFL, the Computing subject Leader, ICT technicians and the head teacher.

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.
- 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.
- All staff, governors and others must only use school based emails (no hotmail or others). Staff must not respond to emails from pupils and or parents directly.
- Emails to parents must be sent via the office and or the head teacher

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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. (Images will show pupil faces but not names)
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Only school cameras and computers should be used to take photos of students.

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

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.
- Staff, governors and other adults will not respond in any way to communication from pupils and or parents through social networking sites, but the school will notify the pupil's parents/carers that they are using such sites.

Managing filtering

- The school will work with the LA, DCFS and the ISP to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site it must be reported to the Online-Safety Coordinator (Computing Subject Leader) or head teacher.
- The Computing subject leader and Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.

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 should only be brought into school by prior arrangement with the head teacher. All mobile phones will be kept in the office during the school day. Pupils found in possession of a phone will have it retained by the head teacher until the end of the school day and may receive a yellow card as a result. They may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff, governors and other adults should not give their personal mobile number to pupils or parents, nor should they use their personal mobile for school business unless previously agreed with the head teacher, this includes email accessed through personal devices such as smart phones or tablets. Staff should switch Bluetooth off from their 'phone when in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.
- All computers, laptops, tablets and storage devices holding personnel and/or pupil data must be password protected. Passwords must not be generic or easily guessed.

Authorising Internet access

Parents will be asked to sign and return a consent form to authorise use of the Internet in school.

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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the Online -Safety policy is adequate and that its implementation is effective.
- The school DSL has signed up to the GSCE website www.gscb.org.uk for notification of updates including Online -safety.
- The Computing subject leader will have regular training in Online -safety policies and practice, which will be logged in the Child Protection file. This training will be disseminated to all staff. See SWgfl website - http://www.swgfl.org.uk/Learning).

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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.
- Parents will be asked to sign and return a consent form to authorise use of the Internet in school.

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 head teacher or the chair of governors.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding 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.

Community use of the Internet

The school will explore the opportunities to liaise with other local schools to establish a common approach to Online -safety.

Delivering Online-safety

Introducing the Online -safety policy to pupils

- Online -safety rules (SMART rules) will be posted in all networked rooms and discussed with the pupils at the start of each year. These rules will be reinforced whenever children use the Internet in school. Parents will also be informed of Online -safety rules and, in signing the Internet Consent form, agree to promote these Online -safety rules when their child uses the Internet outside of school.

- Pupils will be informed that network and Internet use will be monitored. Pupil use of the VLE outside of school will also be monitored, and if necessary, IP addresses will be traced by the Network Manager/Computing Subject Leader in order to identify any a user who has been using the VLE inappropriately.
- As outlined in the National Curriculum, the teaching of Online -Safety will form a key part of the school's planning for each year group.
- The school will make use of pertinent resources and up to date curriculum guidance.

This policy has been reviewed in July 2019

Harewood Junior School

Staff Information Systems Code of Conduct Acceptable use policy

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online -safety policy for further information and clarification.

- I have read and understand my responsibilities under Section 1 and 5 of Keeping Children Safe in Education.
- I understand that Online -Safety is a whole school safeguarding responsibility and I will report any Online -Safety concerns to the DSL.
- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that the school ICT network and associated digital devices/systems may not be used for private purposes without specific permission from the head teacher.
- I understand that the school may monitor my use of the school ICT network and associated digital devices/systems to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission from.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the headteacher or the DSL.
- I will ensure that all electronic communications are compatible with my professional role.
- I will promote Online -safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will not use social networking sites to bring the school into disrepute, discuss or comment on issues relating to the school or pupils or undermine the Teaching/Teaching Assistant Standards.

The school may exercise its right to monitor the use of the school's ICT network and associated digital devices/systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Name(print): …….. Date: ……..

Accepted for school: …….. Name (print): ……..