This policy has been developed to follow the guidelines set by the Gloucester Safeguarding Children Board and has been ratified by Governors. It covers online safety and use of digital media by staff.

This policy will operate in conjunction with other policies including those for Computing, Pupil Online Safety and Computing Acceptable Internet use, Pupil Behaviour, Bullying, Curriculum, Data Protection and Child Protection – along with the Harewood Junior School Staff Handbook.

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
- Promote pupil achievement
- Support the professional work of staff
- 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) - 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 directly to the school's Designated Safeguarding Lead. They must also record any concerns on CPOMS, clicking the 'online safety' box which will also notify the school's Computing Lead, who can take further action as appropriate, in liaison with the school's DSL.

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 above the legal age limit
- Buying age restricted items online
- Hacking and data violations.

Where possible, staff should upload any potential evidence – e.g phone screenshots – as part of their CPOMS recording of the incident.

**Managing Internet Access**

All access to the internet at school is through our certified ISP, SWGfL, which provides firewalls and filtered protection to all pupil internet connections.

- 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**

- The forwarding of chain letters or emails is not permitted.
- All staff, governors and others must only use school based emails for professional communication (no hotmail or others). Staff must not respond to emails from pupils and or parents directly.
- Staff should respect that colleagues may have differing working patterns / hours. As such, this may mean emails being sent and received at a variety of times
- Staff emails 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.
- Each class has a designated class email address as a means of contacting / to be contacted by parents & carers
- Emails to parents & carers must be sent either through designated class email addresses or via the office and/or the head teacher

- Emails to class teachers via class accounts should be in relation to online learning only and all other concerns should be sent to the school office email addresses as usual

**Seesaw – home learning platform**

- Weekly homework is set by class teachers and responded to by children on the Seesaw Home Learning Platform
- There is no expectation for staff to respond to any messages sent via the Seesaw platform outside of normal school working hours
- Parental contact should be through the school office or class email address, as outlined above

**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.
- Staff initials, surnames and job titles will be published on the website.
- The head teacher will take overall editorial responsibility and ensure that content is accurate, appropriate and meets DfE guidelines

**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 school website, particularly in association with photographs
- Only school cameras, iPads or computers should be used to take photos of students – not staff's personal mobile devices
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website during the child's induction into Harewood Junior School

**Social networking and personal publishing**

- The school will block/filter access to social networking sites.
- Newsgroups or chatrooms 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 immediately that their children 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.
- Where certain internet content has been checked by staff, and is deemed of value for pupil's learning, staff are able to access unfiltered internet sites, e.g Youtube, by logging into the network with their personal username and password. All internet activity on this staff network will be monitored to ensure appropriate use at all times

**Managing videoconferencing**

- Where taking part in CPD or communicating with other professionals, staff will maintain a professional conduct and use Google Meet, linked to their school email address, for outgoing calls
- Staff should not use video call to speak directly to individual children unless absolutely necessary, with permission from the headteacher, and with another staff member and/or parent present
- If, in school, a child has an appointment with an external agency virtually via video call, e.g SALT, then a member of staff will be present to supervise and facilitate

**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. Year 6 children may bring mobile phones into school with written permission from their parent / carer. All mobile phones will be kept in the office during the school day.
- Other 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, with their number withheld
- Refer to the Staff Code of Conduct, in the School Handbook, for full guidance on staff mobile phone use

**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 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.

**Authorising Internet access**

- All staff must read and sign the 'Staff Information Systems Code of Conduct Acceptable use policy' 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 if 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.

**Student and supply teacher network and internet access**

- Both student and supply teachers will access school devices through an individually designated log-on credential, e.g Student1, Supply1 etc
- Internet use will be monitored against the username allocated
- The school will keep a record of each supply teacher visit; recording the date, time, network log-on credentials they have used and the class they were teaching in
- Student and supply teachers will not have access to the shared 'Staff Store'. They will be able to access a shared 'STUDENT-GUEST' store to access resources and documents copied over by class teachers as required
- Student and supply teacher network and internet access is subject to the conditions outlined in this policy

**Handling online safety complaints**

- Complaints of Internet misuse will be dealt with by a member of the school's SLT
- 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 and Gloucestershire Police Community Support 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, and the Gloucester School's Partnership network, to establish a common approach to online safety.

**Delivering Online-safety**

Introducing the online safety policy to pupils:

- Online safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Each class teacher will go through every point of the Pupils Acceptable Use policy in their first online safety session in September, to ensure children's understanding and agreement. Children will sign and date the policy, and it will be reinforced and referred to throughout the year.
- In the first half-term of the academic year, teachers will discuss the 'reporting concerns' flowchart and ensure the children know how and where to get help with online safety concerns. This will also be reinforced and discussed throughout the year as needed
- 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 as part of their induction to Harewood Junior School, 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 Seesaw 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 user who has been using Seesaw 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 who will follow the school's Key Skills, Knowledge and Understanding online safety document.
- The school will make use of pertinent resources and up to date curriculum guidance.
- As outlined above, all staff will take a proactive, vigilant and rigorous approach to online safety, immediately reporting any concerns to the school's DSL, and recording details onto CPOMS, ticking the 'online safety' button

- All staff will be familiar with how children can report online safety concerns, on sites such as Childline and CEOP, by referring to the 'HJS Online Safeguarding – Reporting Concerns – Staff Guide'

This policy has been reviewed in June 2022

**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 sections one, two and five 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, and record on CPOMS tagging the 'online safety' button
- 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 the network manager and/or headteacher
- 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 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): ……..