PRENTON HIGH SCHOOL FOR GIRLS

ONLINE-SAFETY POLICY

Owned:	Outcomes and Performance
Reviewed:	Summer 2024
Ratified:	Summer 2024

1 RATIONALE:

Online-safety encompasses the use of new technologies, internet and electronic communications such as learning platforms, wireless and mobile devices, video conferencing, collaboration tools and personal publishing. It highlights the need to educate Students about the benefits and risks of using technology to enable them to control their on-line experiences.

The school's Online-safety policy will operate in conjunction with other policies including Behaviour Policy, Anti Bullying Policy and Data Protection alongside the school curriculum. In particular, staff and students are required to adhere to the school's ICT Acceptable Use Policies (AUP).

1.1 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 the online-safety policy in both administration and curriculum, including secure school network design and use. Safe and secure broadband from an approved Internet Service Provider using suitable filtering.

2 THE ONLINE-SAFETY POLICY

Our Online-safety Policy has been written by the school, building on government guidance. It has been ratified by the school governors. The Online-safety Policy and its implementation will be reviewed regularly.

2.1 Teaching and learning

2.1.1 Why Internet use is 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 is a necessary tool for staff and students.

2.1.2 Internet use to enhance learning

The school Internet access is designed expressly for student use and includes filtering appropriate to the age of students. Students will be offered guidance regarding what Internet use is acceptable and what is not and given clear objectives for Internet use. This is identified in the AUP (Acceptable User Policy) and Home School Agreement.

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

2.1.3 Students will be taught how to evaluate Internet content:

The school will ensure that the use of Internet derived materials by staff and students complies with copyright law. Students are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy. The appropriate use of social media is part of the curriculum for PHSE and ICT Computer Science along with Cyberbullying which is also topic that is covered in lessons and assemblies.

2.2 Managing Internet Access:

2.2.1 Information system security:

- School ICT systems and security will be reviewed regularly.
- The school has an industry recognised internal Firewall along with active virus protection across all school ICT systems.
- The school utilises an automotive auditing server to monitor the core network.
- All connected devices and users are monitored on the ICT network by these security systems

2.2.2 Email:

- Students may only use approved e-mail accounts on the school systems.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Emails sent to an external organisation should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.
- The forwarding of chain emails is not permitted.
- The content of group emails should be relevant to curriculum and school matters.

2.2.3 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 students' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.2.4 Publishing Students' images and work:

Students full names will not be used anywhere on the Website, particularly in association with photographs.

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

Students work can only be published with the permission of the student and parents.

2.2.5 Social networking and personal publishing:

- The school will block/filter access to social networking sites.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Staff will be instructed not to list students as contacts or access students on social networking sites.
- Students and parents will be offered guidance on the use of social network spaces outside school.
- Cyberbullying is included in assemblies and appropriate social media use addressed in form time and during PSHE and ICT/Computer Science Lessons.

2.2.6 Managing filtering:

The school will work with the DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved. Students attempting to access materials, for

example, extremist and indecent images, will be locked out of the internet by the filtering system.

If staff or students discover an unsuitable site, it must be reported to the Online-safety lead Mr Simon. Senior staff will ensure that regular checks are made and the filtering methods selected are appropriate, effective and reasonable.

2.2.7 Managing video conferencing:

IP video conferencing activities, including but not limited to Microsoft Teams, Zoom, Facetime or other platforms will require authorisation from the ICT staff, supervising teacher, and/or the Online-safety lead.

Microsoft Teams is governed by school security policies. Cameras are disabled and not permitted for use by students outside of the school when joining a team session.

Students should ask permission from the supervising teacher before making or answering a video conference call.

Video conferencing will be appropriately supervised for the student's age, and all invitations to any video conference will be done via internal/known school contacts only.

2.2.8 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 during lessons or formal school time for text or voice messages. The sending of abusive or inappropriate text messages is forbidden.

Staff will not use personal equipment or non-school personal electronic accounts when contacting students. Where possible staff will be issued with a school phone where contact with students is required.

2.2.9 Protecting personal data:

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

2.3 Policy Decisions

2.3.1 Authorising Internet access:

- All staff must read and sign the 'Staff AUP' before using any school ICT resource.
- All students and their parents must read and agree to the 'Students' Online-safety Rules (located within student planners in the Home School Agreement section) and AUP.
- Parents will be asked to agree to and sign
  - Student AUP
  - Web publication of work and photographs

The school will keep a central record of all staff and students 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.

2.3.2 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 regularly audit the ICT provision to establish if the Online-safety policy is adequate and that its implementation is effective.

2.3.3 Handling Online-safety complaints:

Complaints of internet misuse will be dealt with by a Behaviour Manager, Online-Safety Lead or Designated Safeguarding Lead. 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 safeguarding procedures.

2.3.4 Community use of the Internet:

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

2.4 Communications Policy:

2.4.1 Introducing the Online-safety policy to Students

Online-safety advice will discussed with the students at the start of each year. Students will be informed that network and internet use will be monitored.

2.4.2 Staff and the Online-safety policy

All staff will be given the School Online-safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

2.4.3 Enlisting parents' support:

Parents' attention will be drawn to the School Online-safety Policy on the school website and via the Parent Bulletin.

2.4.4 Guidance in response to an incident of concern

Risks to Online-safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to Students and in developing trust so that issues are reported. Incidents will vary from a prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police. Misuse can have serious consequences. This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Designated Safeguarding Lead, Online-safety Lead or the Police Liaison Officer.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research:** web sites, search engines and Web browsers
- **Mobile Phones and other mobile devices:**
- **Internet communications:** Email and instant messaging (IM)
- **Webcams and videoconferencing:**

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Bullying and threats
- Identity theft
- Accessing sites that promote extremist views
- Publishing personal information / images
- Hacking and security breaches

How do we respond?

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Designated Safeguarding Lead staff member should be consulted. Relevant policies (Acceptable Use Policy, Behaviour Policy and Anti-Bullying Policy) are referenced and are considered when dealing with the issues identified.

2.4.5 Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme

This will be provided through:

- a discrete programme
- PHSE programmes
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

2.4.6 Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities

- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (guidance contained in the SWGfL Safe Remote Learning Resource)
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

2.4.7 Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

2.5 Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

2.5.1 Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL.org)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Suggested Response to an Incident or Concern