Heathland Whitefriars Federation

ONLINE SAFETY POLICY

Approved by the Board of Trustees: December 2013
Effective from: December 2013

Reviewed 3-yearly by the Safeguarding & Inclusion Committee
Last Review Date: December 2017
Reviewed and Approved by the Safeguarding & Inclusion Committee: February 2021
Next Review Date: December 2023

1. Writing and Reviewing the Online Safety Policy

The Online Safety Policy is part of the school safeguarding agenda and relates to other policies including those for ICT, bullying, Rights Respecting and for child protection.

The school has a designated Online Safety Coordinator who will work alongside the safeguarding co-ordinator to ensure safe usage.

Our Online Safety Policy has been written by the Federation, building on the Harrow Online Safety Policy and government guidance and will be reviewed every 3 years.

2. Teaching and Learning

Article 17: Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need

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 a necessary learning and teaching tool for staff and pupils.

Internet use will enhance learning

The school internet access is subject to rigorous filtering appropriate to the age of the pupils and some content and resources will be prohibited to safeguard staff and pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

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 will be taught to become critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly by the external provider, Beebug, and the Network Manager.
- Virus protection will be updated regularly
- Security strategies will be discussed and dealt with by the in-school Network Manager

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 and this will be recorded by staff on an Online Safety incident log
- Pupils must not reveal personal details of themselves or others in e-mail or any online communication.
- 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.

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.

Publishing images and work

Article 16 Every child has the right to Privacy

- Photographs that include pupils, staff and governors will be selected carefully and will not enable individuals to be clearly identified unless relevant permission is obtained.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

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 should be taught the reasons why personal photographs should not be posted on any social network space without considering how the photograph. 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils must have their parent/carers permission to bring a mobile device to school (Year 6 only).

Dealing with online safety incidents

- Pupils will be taught how to report any online incidents or unsuitable materials that they may come across.
- Pupils and parents who disclose any information about a reported incidence will be kept confidential and only shared appropriately.
- Pupils will be taught who the safeguarding officer (DSL) is in the school and made aware of how to contact her.

Managing filtering

- The school will work with the LGFL, DfE and the Internet Service Provider 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 and recorded on the Online Safety incident log
- Senior staff and the in-school 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 and obtain permission from the supervising teacher before making or answering a videoconference call.
- Video conferencing 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.
- Staff must not use their mobile telephone around children.
- Personal mobile telephones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden and should be reported, logged and followed up by the Online Safety co-ordinator.
- Staff who work across the Federation and are issued with a school mobile telephone should only use for work related communication in a private and confidential manner.

Protecting personal data

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

4. Policy Decisions

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.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to read, sign and return a consent form giving permission for internet access

Assessing risks

- The school will constantly monitor (using external provider Beebug) all ICT access by both Staff and pupils. Any inappropriate content will be reported directly to the Head Teacher.
- 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 will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online 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. Complaints about the Head Teacher must be reported to the Chair of Governors.
- Complaints or incidents will be recorded on an Online Safety incident log.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and referred directly to the Safeguarding co-ordinator.
- Pupils and parents will be informed of the complaint's procedure on the school website and a copy can be obtained from the school office on request.
- Close links and discussions will be held with the local community police to establish procedures for handling potentially illegal issues.

5. Communications Policy

Article 36: Children should be protected from doing things that could harm them

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. Newly arrived pupils will access this information during induction sessions.
- Pupils will be informed that all network activity and online communications will be monitored
- Pupils will be actively encouraged to be vigilant when using devices and immediately report issues that may arise
- Pupils will be made aware and taught how to use the CEOP reporting button located on the school website

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 will be monitored and will be traced to the individual user. Professional conduct is essential at all times.
- Staff should be aware that when unacceptable use is suspected additional monitoring and procedures may come into force.

Enlisting parents' support

Article 16 Every child has the right to Privacy

- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home. Parents will have access to workshops highlighting important Online Safety developments.
- Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school Web site.
- Parents will be made aware and asked to reinforce the use of the CEOP reporting button located on the school website.
- The school operates an open-door policy and would encourage parents to talk to any member of staff if they have any concerns about their child and the use of e safety. The Federation takes Cyber bullying very seriously and will continue to educate the whole school community.
- During school performances some parents have requested for their child not to be photographed. Please respect their right by not filming and taking pictures during this time. Parents will be given the opportunity to take pictures at the end of every performance.