Online Safety Policy

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The ever-changing world of technology highlights the on-going need for children's education on Online Safety

The school's online safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Safeguarding/child protection and Data Protection.

Key Principles

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; 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 internet provision from In4Tech including the effective management of content filtering.

Heaton Park Primary Online Safety Policy

The school has appointed an online safety team. This includes the Designated Safeguarding Lead and the Computing Co-ordinator, as the roles overlap.

The online safety policy will be reviewed annually. This policy will next be reviewed on October 2022.

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. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

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.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access the school's website and Twitter account;
- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and other approved bodies;
- access to learning wherever and whenever convenient.
- Access to remote learning in the event of self-isolation or school closures.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear rules for internet use in and out of school.
- Internet access will be planned to enrich and extend learning activities.
- Staff will monitor and guide pupils in on-line activities that will support learning outcomes planned for the pupils' appropriate level of learning.
- Pupils will be educated in the effective use of the internet in research, including the skills of safety, location, retrieval and evaluation.

Authorised Internet Access

- All staff and pupils will be granted Internet access.
- Pupils and staff will be made aware of the school's rules surrounding internet access and they must adhere to this at all times.
- Staff will have their own log in so that internet activity can be monitored.7
- Staff will adhere to the acceptable use policy
- Pupils will have a class log in and will be heavily supervised when accessing the internet.
- No pupil will be allowed unsupervised access to electronic devices when in school.

Internet Use

- If staff or pupils discover unsuitable sites, the supervising adult must record the URL (address), time, and content must be reported to a member of the online safety team, who will in turn block the site using the ISP filtering.
- Any such incidents must be recorded in an incident log by a member of the online safety team.
- A member of the online safety team must also notify the parents' of pupils involved in such incidents.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy i.e. the use of Wikipedia.

Email

- Staff email addresses are given out by school and must be used for all school related business.
- Personal details will not be sent via email unless to an internal email address or externally by heatonpark@bury.gov.uk.
- Pupils will not have a school email address but will be taught about the use of email and appropriate behaviour when sending emails, within the Computing Curriculum.
- E-mail sent by staff to external organisations should be written carefully, in the same way as a letter written on school headed paper.
- Staff must only open e-mails from a trusted source as this can comprise school data stored on the server.
- The forwarding of chain emails is not permitted.

Social Networking

- Heaton Park Primary and Nursery School does not allow the use of social media within school. Access is blocked via the ISP filtering.
- New social media platforms will be blocked as they arise.
- Staff at Heaton Park Primary School are aware that pupils of all ages are using Social Media Platforms outside of school. Heaton Park Primary School does not condone their use. However, Heaton Park primary School accepts that children will use these platforms and so Online Safety lessons will form an integral part of the Computing Curriculum to ensure that children know how to behave safely online including on Social media Platforms.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised not to place personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Information will be sent out to parents so there is a collaborative approach to safeguarding children online.
- Children are encouraged to talk about the platforms that they are using at home so that staff are aware of what their children are using and can educate themselves and then children on the dangers around using that platform.
- Heaton Park Primary and Nursery School makes use of Twitter as a platform to share highlights within school. No children are identified unless permission is sought from parents prior to the post being made live.

Filtering

- The school will work in partnership with In4Tech and the Internet Service Provider to ensure filtering systems are as effective as possible. Filtering can be updated as and when required in school by the Online safety Coordinator.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and the online safety policy will be amended as appropriate.

Published Content and the School Web Site

- The contact details on the school web site should be the school address, e-mail and telephone number.
- Staff or pupils personal information will not be published.
- The Computing Coordinator and the Administration and Organisation Assistant will take overall editorial responsibility and ensure that content is accurate and appropriate and up to date.

Video and Photography

- Parents will be asked to sign and return a consent form for pupils to have videos and photographs taken for use in school, on the school website, school Twitter and by the local press.
- Names of children will not be placed with videos or photos that are to be published on the school Twitter page or school website. If it is appropriate to identify a pupil, special permission will be obtained from the parent/guardian of the pupil concerned.
- Videos and photographs must only be taken using school equipment.
- Videos and photographs must be stored in 'central' folders on the Teacher Shared area of the school network.
- Once children have left school all relevant videos and photos will be deleted.
- Staff mobile phone use is not permitted anywhere accept office areas and the staff room.
- Pupils must 'hand in' mobile phones into the class teacher at the start of the school day and collect them at the end of the school day. Pupils must not use them whilst on the school premises.
- Parents must sign the agreement regarding pupils bringing mobile phones.
- Staff and pupils must not take photographs or video of colleagues, children or peers on mobile phones, personal cameras or other devices.

Information System Security.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be maintained and updated regularly.
- Security strategies will be reviewed when necessary with guidance being sought from In4Tech, the school's technical support group.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to GDPR rules.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the ISP can accept liability for the material accessed, or any consequences of internet access.
- The school will annually audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

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 of a child protection nature must be dealt with in accordance with school child protection procedures.

Communication of Policy

- Pupils
  - Rules for Internet access will be posted in all working areas.
  - Pupils will be informed that internet use will be monitored.

  Staff
  - All staff will be asked to read the school 'Online Safety Policy'. Its importance will be explained.
  - Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct at all times is essential.
  - All staff, teaching and college students and visitors must agree to adhere to and follow the Staff ICT AUP.
  - All staff, teaching and college students and visitors must agree to adhere to the electronic devices AUP.

Parents and Carers

- Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school Web site.
- Regular updates will also be posted on the school website to support parents and carers in keeping their children safe online.

Preventing Extremism and Radicalisation

At Heaton Park Primary and Nursery School, we recognise how children are vulnerable to influences on the internet, including exposure to extremism and radicalisation. We have a number of steps in place to prevent any inappropriate use.

- School has an appropriate filter on the network, which is provided by the internet service provider. This can be updated with immediate effect.
- All use of the internet is supervised by an adult.
- Access to You tube is blocked for pupil access.
- If inappropriate material does find its way through the filter, children know to turn off the monitor/close the laptop/turn off the screen and report the incident to an adult who will then notify the Online Safety Team immediately.
- Children are taught how to stay safe online. This forms an integral part of our Computing Curriculum and is revisited regularly or as and when is required.