

Online Safety



Reviewed 2015

Next review date 2017



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

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 Bury LA including the effective management of content filtering.

Online safety Audit

This quick self-audit will help the online safety team to review whether the online safety policy is effective.

Date of last update:	
The policy was agreed by governors on:	
The policy is available for staff from Head Teacher or Teacher Shared Area on the school network	
And for parents on school website	
The designated Child Protection Officers are: Mr Lord & Mrs Brignall	
The online safety team is: Mr Lord, Mrs Brignall & Miss Harper	
Has online safety training been provided for both pupils and staff recently?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the school online safety rules?	Y/N
Have school online safety rules been set for pupils?	Y/N
Are these rules displayed in all rooms with computers?	Y/N
Is the internet access provided by an approved educational Internet service provider.	Y/N
Has the school filtering policy has been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Heaton Park Primary Online Safety Policy

The school has appointed an online safety team. This includes the Designated Child Protection Officer as the roles overlap and the Computing Co-ordinator.

Our online safety policy has been written by the online safety team with guidance from Bury LA's 'Digital Safety in Bury Schools' document. It has been agreed by the senior management team and approved by governors.

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

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 blog;
- 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.

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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should 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 (subject to parental consent) will be granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- 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 report the details to the TCSC.
- 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.
- School will ensure that the use of Internet derived materials by pupils and staff will respect copyright laws.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use learning platform e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff and pupils must only open e-mails from a trusted source.
- The forwarding of chain letters is not permitted.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups 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 advised not to place personal photos on any social network space.
- Pupils should 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.

Filtering

The school will work in partnership with the Local Authority, e-Safe and the Internet Service Provider to ensure filtering systems are as effective as possible.

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 and learning platform should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

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 and by the local press.
Names of children will not be placed with videos or photos that are to be published on the learning platform 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 phones will not be used during lessons.
- Pupils must 'hand in' mobile phones into the school office at the start of the school day and collect them at the end of the school day.

- 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 the LA and/or the school's technical support group.

Protecting Personal Data

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

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 Bury LA can accept liability for the material accessed, or any consequences of Internet access.
- The school should 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 headteacher.
- 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 networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils must agree to sign and follow the Pupil ICT Acceptable Use Policy.

Staff

- 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 at all times is essential.
- All staff, students and visitors must agree to sign and follow the Staff ICT AUP.
- All staff, students and visitors must agree to sign the electronic devices AUP.

Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.
- A leaflet will also be sent home to inform parents on how to keep their children safe online.

Preventing Extremism and Radicalisation

At Heaton Park 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 Bury LA
- All use of the internet is supervised by an adult
- Access to You tube is supervised by an adult
- If inappropriate material does find its way through the filter, children know to turn off the monitor and report the incident
- Children are taught how to stay safe online