Pudsey Bolton Royd Primary School

'Succeed today,

prepare for tomorrow'

'A happy, welcoming, school community where we all engage, achieve and excel.'

Internet Access Policy
Academic Year 2017 - 2018

Rationale

Access to the Internet is a necessary tool for all staff and students irrespective of gender, race, religion, culture or ability. It is an entitlement for students who show a responsible and mature approach with the intention to gain useful or entertaining resource.

The purpose of internet access in school is to raise educational standards, to support the professional work of the staff and to enhance the schools management information and business administration system. Access to the internet is a necessary tool for all staff and children, the benefits include;

Resources

♦ Providing access to documentation including on-line publishing of documents (schools' policies, lesson plans, activities, etc)

♦ Access to world-wide educational resources.

♦ Inclusion in government initiatives.

♦ Information and cultural exchanges between students worldwide

♦ Discussion with experts in many fields for pupils and staff

Staff Professional Development

♦ Access to educational materials

♦ Sharing good practice with colleagues

♦ Communication with the advisory and support services, professional association and colleagues

♦ Developing pupils/staff personal skills in ICT

Administration

- ♦ More regular communication with schools and more immediate responses to inquiries
- ♦ Improves access to technical support including remote management of networks
- ♦ Method to publish information to schools that will free more resources for teaching and learning
- ♦ Management of the school network from a single source, thus reducing the overall cost of performing this role
- ♦ Added value through access to Council IT systems (e.g. finance and payroll)
- ♦ Added value through the creation of a secure effective communication system between schools and the LEA and between each other that can improve the transfer of information and data.

Email

- ♦ Provision of a quick method of communication between pupils, staff and officers of the authority
- ♦ Provision of a centrally maintained email system that can give pupils an email address that will remain constant throughout their education in any Leeds school.

Security

- ♦ Provision of a buffer between Leeds schools and the Internet designed to both protect users and enhance performance
- ♦ Secure filtered Internet access
- ♦ Filtered email for staff and pupils
- ♦ Email anti-virus – scan all unencrypted external and internal email delivered to Leeds Learning Network, using anti-virus system that are kept constantly up to date
- ♦ Sophos anti-virus distribution – community license, supply software media and documented instructions to enable the School ICT Support to deploy and maintain Sophos anti-virus software on all its servers (however it is the school's, technicians and individual staff responsibility to ensure their servers, laptops and workstations are constantly updated)
- ♦ Microsoft Critical Updates: distribution of Microsoft critical security updates services SUS and MSUS (school's responsibility to ensure computers are kept updated)
- ♦ Statutory UK ISP monitoring laws – Records all Internet usage and email. The Head Teacher of the school will be informed regarding any relevant issues.

<u>Equal Opportunities</u>

School will ensure that all our children irrespective of race, gender, or ability/disability will have access to the internet through the following;

- Computing coordinator and technician will liaise with class teachers and SENCO to ensure that specialist equipment is purchased and deployed as required.
- School technician will liaise with class teachers and SENCO to make adjustments to screen displays, text size and mouse icons as deemed necessary.
- Class teachers will be responsible ensuring that the content accessed on the internet is accessible and suitable for all individuals.

Safe Internet Access

Access to appropriate information should be encouraged and Internet access must be safe for all members of the school community from youngest pupil to teacher and administrative officer. School's blocking system assigns rights based on their log on credentials setting different levels of filtering for staff and pupils. The filtering software used as part of the ISP contains a number of lists or categories of URLs that can be marked as allowed or denied. These lists are updated frequently. Through these categories a filtering policy has been established for groups of users. These groups are arranged by age and organised by Key Stage. Teachers might need to research areas including drugs, medical conditions, bullying or harassment. In such cases, legitimate use must be recognised and the user protected from possible accusation of inappropriate use. The disallowed categories are assigned to each Key Stage. Sites that are within disallowed categories are blocked automatically. This mechanism provides an additional 'safety' check. It also allows for many more sites than it would conventionally be available using the simple 'allowed list' system used by other filtering applications. None of these systems can be completely effective in isolation therefore a combination of approaches is used. It is acknowledged that adequate supervision is essential as well as teachers proactively engaging children in weekly online safety discussions so they know what to do in such instances.

If staff or pupils discover unsuitable sites, the URL address and content must be reported via the computing co-ordinator or school technician; where minority languages are involved, appropriate measures will be used to ensure the process to select appropriate material is adequate.

To ensure safe internet access;

♦ Pupils and staff will be informed that Internet use will be supervised and sites selected will be monitored

♦ Users will inform the computing co-ordinator if their password is being used by another person or has been lost

♦ The school will work in partnership with parents, Children Leeds, DfES and ICT4Leeds to ensure systems to protect pupils are reviewed and improved.

Teaching and Learning

To effectively and safely use the internet to enhance learning

- ♦ Internet safety will be taught explicitly weekly.
- ♦ Internet access will be planned to enrich and extend learning activities
- ♦ Pupils are given clear objectives for their internet use
- ♦ Staff select sites which support the learning for pupils' age and maturity
- ♦ Pupils are taught how to take responsibility for their own internet access
- ♦ Pupils are taught how to evaluate and ways to validate information and internet content before accepting that it is accurate.
- ♦ Pupils are taught to acknowledge the source of information in their own work.
- ♦ Pupils are made aware that the writer of an e-mail of the author of a web page may not be the person they claim to be.
- ♦ Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Managing Internet Access

Authorising Web Access

♦ All staff must read and sign the "Code of Conduct" before using any ICT source.
♦ Parents are asked to sign a consent form regarding their child's internet use.
♦ Any person not directly employed by the school will be asked to sign and read the "Code of Conduct" before being allowed access to the internet.
♦ Internet access and email content will be automatically monitored.

E -mail

♦ E-mail must only be sent and received via schools official email addresses.
♦ E-mail via schools systems must only be used in school for work related purposes
♦ Key stage 1 pupils may send email as part of planned lessons but will not be given individual email accounts
♦ Key stage 2 pupils will be given individual email account. This assumes a high level of trust and pupils will be asked to sign the 'Rules for Responsible Internet Use Statement'(pupil planner, appendix for staff)
♦ In-coming and outgoing email will be regarded as public and will be monitored
♦ Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper
♦ The sending of any sensitive personal data by pupils, for example home address, photographs or telephone numbers relating to the user or any other person is forbidden and is to be addressed in weekly online safety lessons.
♦ Users will be held responsible for email sent from their account

Web publishing

A website can commemorate pupils' work, promote the school and publish resources for projects or homework. The website must reflect the school ethos and ensure the information is accurate and well presented. As the school's website can be accessed by anyone on the Internet, the security of staff and pupils must be considered carefully. The ICT4Leeds, School or the council ***will not be made liable*** under any circumstances for any injury, distress, loss or damage to the pupil or parents who may arise directly or indirectly from the publishing of information on the website.

♦ The Head Teacher will delegate editorial responsibility to a member of staff or other responsible person(s) to ensure that content is accurate and quality of presentation is maintained
♦ The school website will comply with the school's guidelines for publications
♦ Pupils will be made aware that work published on the internet will be viewed by a diverse range of people.
♦ Teachers will be encouraged to select and publish work to reflect the successes and achievements of the individual.
♦ All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name
♦ The point of contact on the website should be the school address and telephone number. Home information or individual email identities will not be published
♦ Photographs must not identify individual pupils. Group shots or pictures taken over the shoulder will be used in preference to individual "passport" style images. Full names will not be used anywhere on the website, particularly alongside photographs
♦ Written permission from pupils and their parents will be sought before any personal data e.g. names and photographs of pupils are published on the school website.

Cyber Bullying

The school treats very serious any incidence of cyber bullying whether inside or outside of school. Children will be encouraged to tell a teacher if they encounter any material that makes them feel uncomfortable.

Social networking and managing video conferencing
♦ Pupils will not be allowed to access public chat rooms without supervision and are only allowed to use sanctioned sites.
♦ New applications will be thoroughly tested before pupils are given access.
♦ Video conferencing and web cams must only be used when sanctioned by a member of staff and pupils must follow the school's Behaviour Policy.
♦ Video conferencing and web cam use is always appropriately supervised and pupils must ask permission before accepting or making any calls.

Risks Assessments

School has put in place mechanisms to make Internet Access as safe as possible. However, the school needs to be aware that the nature of the Internet and its changing content makes it impossible to guarantee that all risk is removed. It is essential that good practice is developed within school to minimise risk, by viewing sites that are knowingly going to be used before a lesson, as well as checking that the filtering and blocking mechanisms are working and reporting inappropriate content to the helpdesk as soon as possible.

Pudsey Bolton Royd School Statements:

In common with other material such as magazines, books and videos, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the International scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Neither School nor Leeds City Council can accept liability for the material accessed, or any consequences thereof:

- The use of computer systems without permission or of purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken
- The Head Teacher will ensure that the policy is implemented effectively
- The school will abide by the Data Protection Act 1998

See appendix a: Statement

ICT Security Statements:

- Security strategies as discussed with the LEA will be implemented
- The ICT co-ordinator/ network manager will ensure that the system has the capacity to take increased traffic caused by Internet use
- The security of the whole system will be reviewed with regard to threats to security from Internet access
- Personal data sent over the Internet will be encrypted or otherwise secured
- Virus protection will be installed and updated regularly
- Use of pen drives will be reviewed. Personal pen drives may not be brought into school without specific permission and a virus check
- Use of email to send attachments such as system utilities will be reviewed

Internet Complaints Procedures

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the issue has arisen through Internet use inside or outside school. The school will need to discuss procedures for dealing with transgressions and these may be linked to the school's behaviour/ disciplinary policies. Transgressions of the rules may be minor, whereby a temporary ban on Internet use will be adequate or major where an investigation may take place. Serious cases may necessitate the involvement of the local authority officer or the police.

School Statements:

♦ Responsibility for handling incidents will be given to senior members of staff
♦ Pupils and parents will be informed of the complaints procedures
♦ Parents and pupils will need to work in partnership with staff to resolve issues
♦ As with drugs issues, there may be occasions when police must be contacted. Early contact will be made to establish the legal position and discuss strategies
♦ Sanctions available for pupils include interview/counselling by Head Teacher and if appropriate, informing parents or carers
♦ A pupil may have email, Internet or computer access denied for a period of time depending on the nature of the incident

Review of the Policy

The Internet access Policy has been written by a team with a wide range of experience and will be reviewed on a yearly basis. It has been discussed with all staff, agreed by the senior management and approved by governors.

Revised: March 2016

Originally created by: Head Teacher, Deputy Head Teacher, ICT Coordinators and School technician

Revised by Computing Coordinator – March 2016 Paul Kilner

Review date: December 2017