E-Safety Policy

Barndale House School

E-Safety

The aim of this E-Safety Policy is to ensure that pupils will benefit from learning opportunities offered by the school's internet resources and other new technologies in a safe and effective manner. It highlights the need to education pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The E-Safety Policy is part of the school development plan and relates to and acts in conjunction with other policies including those for ICT, student behaviour, bullying, child protection, data protection and security.

The E-Safety policy has been written by the appointed E-Safety Co-ordinator (Mrs Helen Hemsley), building on current Government and LEA guidance. It has been agreed by senior management and approved by the governing body. The E-Safety policy and its implementation will be reviewed annually.

Teaching and Learning

Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with appropriate, quality internet access as part of their learning experience. 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 functions.

Barndale School employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the internet

- Pupils' use of the internet will always be supervised by a member of staff
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils
- Staff will guide pupils in on-line activities that will support learning outcomes planned in accordance with their age and ability
- Pupils will be guided as to what internet use is acceptable and what is not and given clear objectives for internet use
- Internet access will include appropriate filtering to minimise the risk of exposure to inappropriate material
- Teachers and pupils will be provided with appropriate training in the area of internet safety

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law
- Where appropriate, pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- Where appropriate pupils will be taught to be critically aware of the materials they access and shown how to validate information before accepting its accuracy
- Uploading and downloading of non-approved software will not be permitted
- The use of personal floppy discs, memory sticks, CD Roms or other digital storage media in school requires permission from a member of staff.

Managing Information Systems

- An audit and review of the school ICT provision and security strategies will be conducted regularly by the SMT
- Security strategies will be discussed with Northumberland LEA Computer Services to ensure systems to protect pupils are regularly reviewed and if necessary improved
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- The school complies with the LA security strategies. PCE is used on all education computers including staff laptops
- Virus protection will be updated regularly
- Personal data taken off site will be encrypted
- Unapproved software will not be allowed in work areas or attached to email
- Files held on the school's network will be regularly checked
- If staff or pupils discover an unsuitable site it must be reported to the E-Safety Co-ordinator
- The school will block access to social networking sites
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

E-mail

- Pupils may only use approved e-mail accounts on the school system under supervision of a member of staff and solely for school purposes

- Sending and receiving e-mail attachments is subject to permission from a member of staff
- Pupils must immediately inform a member of staff if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission
- Email sent to an external organisation should be written carefully and authorised before sending
- Pupils will only have access to chat rooms, discussion forums, messaging or other electronic communication forums that have been approved by the school. Such usage will be for educational purposes only and will always be supervised
- Staff will only use official school provided email accounts to communicate with parents/carers as approved by the SMT
- Access in school to external personal email accounts may be blocked
- Staff should not use personal email accounts during school hours or for professional purposes.

School Websites

- Staff or pupil personal information will not be published on any website without permission
- Pupils will be given the opportunity to publish projects, artwork or school work on the world wide web in accordance with clear policies and approval processes regarding the content that can be uploaded
- The Headteacher will take overall responsibility for online content published by the school and will ensure that content published is accurate and appropriate
- The publication of pupils' work will be co-ordinated by a member of staff
- Pupils' work will only be published with the permission of the parents/carers
- Written permission from parents or carers will be obtained before photographs of pupils are published on a website
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

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

- The school will control access to social media and social networking sites
- Pupils will be advised on security and privacy online
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's Acceptable Use Policy

Filtering

- The school's broadband access will include filtering appropriate to the age and abilities of the pupils
- The school will work with Northumberland Education Services and Computer Services to ensure that the filtering policy is continually reviewed
- The school has a clear procedure for reporting breaches of filtering. All members of the school community are aware of this procedure
- The school filtering system blocks all sites on the Internet Watch Foundation list.

Protecting Personal Data

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

Policy Decisions

- All staff must read and sign the Staff Information Systems Code of Conduct before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are granted access to the school ICT systems
- Parents will be asked to read the School Acceptable Use Policy
- Parents will be asked to sign and return an internet use consent form.

Risk Assessment

- The school will take 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. Neither the school nor Northumberland LEA can accept liability for the material accessed or any consequences of Internet access
- The school will audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective

- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling Concerns

- All members of the school community will be informed for the procedures for handling concerns
- The E-Safety Co-ordinator will record all incidents and actions taken

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by the SMT in accordance with the school's complaints procedure
- 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
- All complaints and incidents will be recorded by the school including any actions taken
- Pupils and parents will be informed of the complaints procedure.

Cyberbullying

- Cyberbullying will not be tolerated. Procedures are in place to support pupils affected by cyberbullying
- All incidents of cyberbullying will be reported, recorded and investigated.

Learning Platforms

- The SMT and staff will monitor the use of learning platforms
- Pupils and staff will be advised of acceptable conduct and use
- Only members of the current pupil and staff community will have access to the learning platform.

Mobile Phones

- Mobile phones will not be used during lessons or formal school time
- The sending of abusive or inappropriate text messages is forbidden
- If a pupil needs to contact their parents during school time they will be allowed to use a school phone
- Staff are not permitted to use their own personal phones to contact parents/carers

- Staff will not user personal devices to take photos or videos of pupils.

Communications Policy

- E-Safety rules will be posted in all ICT areas and regularly discussed with the pupils
- Pupils will be informed that computer and internet use will be monitored
- All staff will be given the School E-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.
- Parents' attention will be drawn to the school E-Safety Policy.

Helen Hemsley