Mountbatten Online Safety Policy **January 2019**

Teaching and learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning. The school internet access will be monitored for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for its 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 shown how to publish and present information to a wider audience.

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 how to report unpleasant internet content.

Managing internet access

School ICT systems security will be reviewed regularly within the school and by Ian Pollard (group IT consultant). Virus protection will be updated regularly. Security strategies will be discussed with the internet provider.

The school works with Ian to ensure systems to protect pupils are continually reviewed and improved. Smoothwall is in place to support filtering of websites and reports are sent to the Online Safety Coordinator. If staff or pupils view unsuitable on-line materials, the site must be reported to the Online Safety Coordinator. Checks are made to the filtering methods in order they are appropriate, effective and reasonable.

Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and students.

Serious incidents involving radicalisation have not occurred at Mountbatten to date. However, it is important for us to be constantly vigilant and remain fully informed about issues that affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation ‘could not happen here’ and to refer any concerns through the appropriate channels (currently via the Child Protection/ Safeguarding Coordinator).

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Hull City Council can accept liability for any material accessed, or any consequences of Internet access.

Mountbatten audits ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Staff will always use a child friendly safe search engine when accessing the web with pupils, safe search engines include:

- www.bing.com;
- www.safesearch.com
- www. pawsexplore.com.

Authorising Internet access

All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. At Key Stage 2, access to the Internet will be directly supervised access to specific, approved on-line materials.

On entrance to the school, parents will be asked to read, sign and return a Rules for Responsible Internet Use consent form. The Rules for Responsible Internet Use will be shared with all pupils and will be referred to during the use of the internet in lessons.

Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. Pupils will be informed that network and Internet use will be monitored and appropriately followed up. Online Safety training will be embedded within the ICT scheme of work for pupils. Staff will receive regular training in Online Safety.

All staff will be given the School e-Safety Policy and its importance explained. Staff must be informed that network and internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

E-mail

Pupils may only use the approved itslearning e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. E-mails from pupils to external bodies are presented and controlled by the internet filter, the class teacher or the admin staff.

Mobile technology

All mobile technology will be password / code protected to comply with safe guarding regulations. The Ipad trolleys are kept in a secure strong room at the end of each day. The key for the Ipad trolleys are stored in the EYFS staff room (KS1 trolley) and in the main school office (KS2 trolley)

Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Staff should consider using group photographs rather than full face photos of individual children. Photographs of pupils must only be used on the school website and/or Twitter if parent/carers have given consent for this. Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.

Social networking

The school will control access to social networking sites, and ensure that opportunities are provided in Computing and PSHE lessons to educate pupils in their safe use. Pupils will be told to never give out personal details of any kind, which may identify them, their friends or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Protecting personal data

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

All USBs and mobile storage devices used within the school and contain children's personal data or assessment information must be encrypted.

The head teacher and computing coordinator will take overall editorial responsibility for the school website and ensure that content is accurate and appropriate. Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team
- 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
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

This policy will be reviewed annually.

Date Reviewed: January 2019
Policy reviewed by: Melanie Legg
Date approved by the Governing Body: 12/2/19
Review Date: January 2020