Hardy Mill Online Safety Policy

Introductory Statement

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Use of email, mobile phones, Internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources.
- Virtual Learning Environments (VLEs) provide children with a platform for personalised and independent learning.

Dangers associated with the Internet and emerging new technologies.

- Children might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful electronic messages.
- Children might receive unwanted or inappropriate messages from unknown senders via email or instant messenger. They might also be exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites, such as Facebook, Twitter, Instagram etc.
- Chat rooms provide cover for unscrupulous individuals to groom children.

Social and educational benefits to be derived

- Children are equipped with skills for the future.
- The Internet provides instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's reading and research skills.
- Email, Instant Messaging and Social Networking helps to foster and develop good social and communication skills.

It is important to note that these far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

This policy focuses on each individual technology available within the school and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to. These safety guidelines are provided to enable pupils and staff to be responsible for their own internet use and browsing behaviour.

Procedures for Use of a Shared School Network

This section outlines what users must and must not do when using a PC / laptop / tablet connected to the school network.

- Users must access the school network using their own logons and passwords. These must not be disclosed or shared.

- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.

- Software should not be installed, nor programmes downloaded from the Internet, without prior permission from the person responsible for managing the network.

- Removable media (e.g. pen drives / memory sticks and CD-ROMs) must be scanned for viruses before being used on a machine connected to the network.

- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer' or Windows key+L).

- Machines must be 'logged off' correctly after use

- The wireless network must be password protected to prevent outsiders from being able to access it.

Procedures for Use of the Internet and Email

Outline of the procedures for safe Internet and Email use as agreed by Hardy Mill Primary School.

- All users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment. These must be completed at the start of each academic year. All forms are to be stored centrally in the school office.

- Parental or carer consent is required in order for children to be allowed to use the Internet or email.

- The Internet and email must only be used for professional or educational purposes.

- Children must be supervised at all times when using the Internet and email. Children are advised to tell an adult if they accidently open an image or click on an inappropriate pop-up.

- Accidental access to inappropriate, abusive or racist material is to be reported without delay to the Headteacher and a note of the offending website address

(URL) taken so that it can be blocked. These details should be recorded on an Online Incident Form (which can be found in office 365). The internet service is provided by Bolton council and software is used to monitor and control website access.

- Internet and email use will be monitored by Bolton council regularly in accordance with the Data Protection Act.

- Users must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.

- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- All emails sent from a school email account will carry a standard disclaimer disassociating the school and the Local Authority with the views expressed therein.

- Bullying, harassment or abuse of any kind via email or instant messenger will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- If users are bullied, or offensive emails/instant messages are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails/messages received should not be deleted, but kept for investigation purposes.

- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.

- Users must seek permission before downloading any files from the Internet.

- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

<u>Procedures for Use of Instant Messaging (IM), Chat and Weblogs</u>

- The use of Instant Messaging (e.g. Facebook messenger or Whatsapp) is not permitted on school devices.

- Use of Social Networking websites, such as Instagram, Facebook, Twitter is not permitted.

- Children and staff must not access public or unregulated chat rooms on school devices.

Procedures for Use of Cameras, Video Equipment and Webcams

- Permission must be obtained from a child’s parent or carer before photographs or video footage can be taken. If parents wish to take photographs during a performance, they must sign a disclaimer, which will be kept on file.

- Photographs or video footage will be downloaded promptly and saved into a designated folder. This will be accessible only to members of staff.

- Any photographs or video footage stored on cameras should be deleted promptly once footage and photos have been downloaded. Staff should save them to the designated folder on the school server.

- Adults should use school cameras or iPads to photograph or record pupils during school trips or visit and should transfer and save images and video footage into the designated folder on a school computer promptly upon their return.

- Webcams must not be used for personal communication and should only be used with an adult present.

- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of the school’s website

- The Headteacher is responsible for approving all content and images to be uploaded onto its website prior to it being published.

- The school website should be subject to frequent checks to ensure that no material has been inadvertently posted, which might put children or staff at risk.

- Copyright and intellectual property rights must be respected.

- Permission must be obtained from parents or carers before any images of children can be uploaded onto the school website.

- Names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.

- When photographs to be used on the school website are saved, names of individuals portrayed therein should not be used as file names.

Procedures for using mobile phones

- During COVID19 restrictions, pupils will not be permitted to bring a mobile phone to school.
- Once COVID19 is no longer a risk, the following procedures will resume:
  - Mobile phones belonging to pupils must be switched off whilst on school premises.
  - Year 5 and 6 children may bring mobile phones into school - phones must be signed into the the mobile phone log books in their classroom upon arrival, after which they will be sent to the office and stored securely for the duration. They will be kept in the school safe, until the child collects the phone at home time.
  - All staff must ensure that their mobile phones are available to receive messages from the school office during the school day. Staff should use their mobile phones to respond to office messages to reduce unnecessary contact with other staff members. Personal messages should be responded to at break and lunch times, away from pupils.

Procedures for using wireless gaming devices

Not only might their presence lead to instances of theft, but as children can also connect to the Internet and play against other people online, they represent the same dangers as public chat rooms

- Their use by children is not permitted at Hardy Mill during school hours (8:50-3:30). The use of a games console that is **NOT** connected to the internet is permitted, during breakfast club hours and in after school club. Online educational games that have been verified, are allowed.

Procedures for Use of Showbie and Taspesty at VLEs

Outline of the procedures for safe VLE (virtual learning environment) use as agreed by Hardy Mill Primary School. For additional information regarding remote learning through a VLE, please see the Remote Learning Policy.

- Weekly homework will be set on showbie, which pupils will have access to through their own unique username and password.
- Pupils should not share their username and password with others.
- Should pupils forget their login details, staff will be able to reset these details to pupils can access learning at home
- Pupils are expected to behave responsibly on their VLE, using manners which we would expect to see in school.
- If pupils have difficulty accessing activities on their VLE, parents or carers should email their child's class teacher for guidance.

Sanctions to be imposed if procedures are not followed

- Letters may be sent home to parents or carers (if applicable)
- Parents or carers may be contacted by telephone
- Users may be suspended from using the school’s computers, Internet or email, etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious cases.

Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the school and that this policy will not remain static. It may be that staff / children might wish to use an emerging technology for which there are currently no procedures in place. It is therefore advisable to state that the use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

This Policy was agreed by the Governing Board: 22nd November 2016

It will be reviewed: Annually

Named Governor: Mr Andrew Hall

Named Staff member: Mrs Rebecca Southworth

Reviewed: November 2020