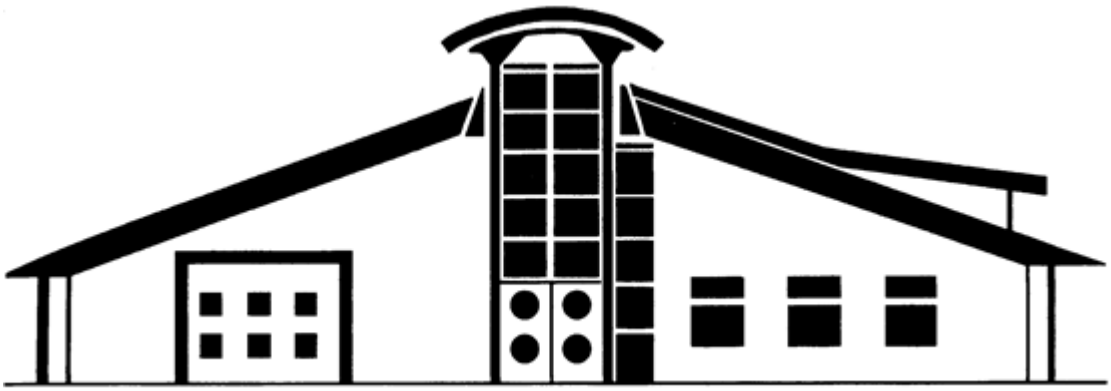
HOLMESDALE COMMUNITY INFANT SCHOOL



E-SAFETY POLICY

Agreed by Staff .....May 2023

Approved by Governors.....July 2023

Review Date .....May 2024

Holmesdale School E-Safety Policy

Writing and reviewing the e-Safety policy

E-safety is part of the school's safeguarding responsibilities. This policy also relates to other policies including those for Behaviour, Safeguarding, Anti-bullying, GDPR/Data Protection and Acceptable Use.
Holmesdale Infant and Nursery School is committed to ensuring that everyone in school is able to operate with safety and confidence whenever and wherever they use the Internet or mobile technologies.

What is e-Safety?

E-Safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate children about benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Using this policy

- The school has an e-safety co-ordinator (Sharon Mullarkey)
- The e-safety policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by Governors
- This e-safety policy was revised by: Sharon Mullarkey
- This e-safety policy and its implementation will be reviewed annually. The next view is due: Summer 2024
- This e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site
- This e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff/pupil

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience
- Internet use is a part of the curriculum and a necessary tool for staff and pupils. Eg. email, research, lesson resources, online programmes etc.
- Internet use will enhance learning
- The school Internet access includes 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 Internet use
- Pupils will always be supervised and directed when using the internet in class.
- 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 appropriately to a wider audience.
- Pupils will be taught how to evaluate Internet content
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law

- Pupils should be taught to be aware of what they are reading and its validity
- Pupils will be taught how to report unpleasant Internet content by telling an adult in their class

IT Safety and Data protection

The school will provide managed internet access to its staff and pupils to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside of the school network

- The school will have up-to-date virus and anti-spam protection, and any suspicious activity or threat should be reported to SLT
- Access to school networks will be controlled by secure passwords. There are automatic prompts set up to ensure that these are up-dated three times a year
- The school will look to improve security passwords where practicable, for example roll out of Multi Factored Authentication passwords
- The security of school IT systems will be reviewed weekly by our IT technician and remedial action will be taken immediately to maintain the integrity of the network and services
- Staff will not install any software on to school computers without authorisation given by the Headteacher, or Computing Co-ordinator (L. Hughes)
- USB storage drives are not permitted for use on school equipment
- The school assesses the risks to ensure the safe and secure storage and use of personal data within the school
- Personal data will be stored securely on-site and, in the cloud, and backups will be kept according to the best practice of 3-2-1 (**three** copies of the data exist at any one time, the data is kept on **two** different types of storage media and **one** copy of the data is sent off site)
- It should be possible to recover core systems and data for a minimum period of 90 days

Internet Use

- The school will use a recognised internet service provider or regional broadband consortium – our current provider is Zen Internet
- The school will ensure that all internet access has age-appropriate filtering and monitoring provided by a recognised provider – our current provider is Untangle
- A member of the SLT should set the categories for blocking and alerting
- Systems will be in place to ensure that internet use can be monitored, and a log of any incidents will be kept to identify patterns of behaviour and to inform e-safety policy
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored
- Real-time alerts are sent to a member of the SLT when a category within the KCSiE list is accessed
- It is vitally important that staff are careful about content that they search for or download. Every time a page is viewed on the internet, it is possible to trace that visit back to the school computer. This means that it is possible to tell if a school computer was being used to look at inappropriate web pages

- The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety
- All communication between staff and pupils or families will take place using school equipment and/or school accounts
- Pupils will be taught not to give out personal details or information which may identify them or their location

E-mail

- Staff may only use approved e-mail accounts on the school IT systems – our current provider is Microsoft 365
- All incoming and outgoing emails can be traced within the 365 admin portal. This is a data protection and compliance requirement, and commonly used for subject access requests
- Great care must be taken when sending emails containing confidential information outside of the school network; only initials will be used to identify children unless the email is being sent via

  the encrypted messaging system, 'Egress'
- Incoming email should be treated as suspicious, and attachments **must not be** opened unless the author is known.
- Governors provided with Holmesdale e-mail accounts to use for all school committee communications
- Staff and Governor leavers will not have access to their school e-mail account after their last day. The email will be accessible by the school if required for 30 days after their leaving day, after this it will be permanently deleted
- School email accounts will be protected by Multi Factor Authentication

Published content e.g. school web site, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website

Assessing Risk

- A record of all staff accessing our IT system will be kept and all members of staff will acknowledge they have read and agreed to adhere to our acceptable use policy/code of conduct.
- The school will take all reasonable precautions to prevent access to inappropriate material Internet usage is monitored, 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

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- 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 and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy to staff

- All staff will be shown where to access this e-safety policy and its importance explained
- All staff will receive e-safety training

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school
- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, and on the school web site
- Parents will be signposted to organisations and information to support their child's safety online