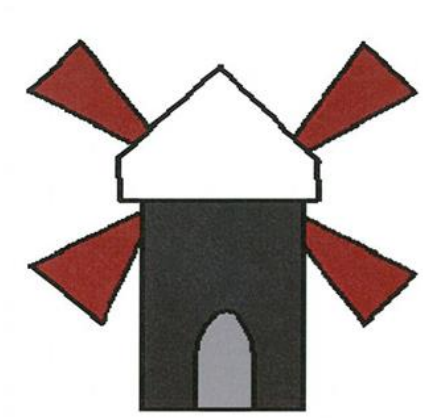
Holland Moor Primary School,
Cornbrook, Skelmersdale



INTERNET SAFE USE POLICY

Holland Moor Primary School

Bringing Out The Best

E-Safety Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users- refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with legal responsibility for your child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents and visitors.

Safeguarding is a serious matter; at Holland Moor Primary School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.
The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foresee ability of harm to the student or liability to the school.

This policy is available for anybody to read on the Holland Moor Primary School website; upon review all members of staff will sign as read and understood both the e-safety and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.
Head Teacher Name: Mr M Beale

Chair of Governors: Mrs B Trainor

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.
    - Chair the E-Safety Committee.

Head Teacher

Reporting to the governing body, the Head Teacher has overall responsibility for e-safety within our school. The day-to-day management if this will be delegated to a member of staff, (or more than one), as indicated below.

The Head Teacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The day-to-day of e-Safety Officer is devolved to Anna Ainscough.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head Teacher.
- Advise the Head Teacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, ICT technical support and other agencies as required.
- Retain responsibility for the e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Head Teacher and responsible governor to decide on what reports may be appropriate for viewing.

- **ICT Technical Support Staff**

Technical support staffs are responsible for ensuring that:

- The ICT technical infrastructure is secure; this will include at a minimum:
-
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
  - Any e-safety technical solutions such as Internet filtering are operating correctly.
  - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Head Teacher.
  - Passwords are applied correctly to all users regardless of age Passwords for staff will be a minimum of 8 characters.
  - The ICT System Administrator password is to be changed regularly.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Head Teacher. If you are unsure the matter is to be raised with the e-Safety Officer or the Head Teacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, School website and VLE the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.
Parents must also understand the school needs have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Holland Moor Primary School uses a range of devices including PCs, laptops, iPads, iPods and Kindle Fire. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology.

Internet Filtering – we use Netsweeper software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, E-Safety Officer and ICT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher.

Email Filtering – we use Netsweeper software that prevents any infected email to be sent from the school or the be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head Teacher immediately. The Head Teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
(*Note: Encryption does not mean password protected).*

Passwords – all staff and students will be unable to access any device without a unique username and password. The ICT Coordinator and ICT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. ICT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.
Students are permitted to use the school email system, and as such will be able to access their class email address. The email address will be made up of their class name e.g. class2b@hollandmoor.lancs.sch.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – There are many social networking services available; Holland Moor Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Holland Moor Primary School and have been appropriately risk assessed; should staff wish to use other

social media, permission must first be sought via the e-safety Officer who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school on Moodle.
- Twitter – used by the school as a broadcast service (see below),
- Facebook – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permissions slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents – Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Head Teacher. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum – It is important that the wider school community is sufficiently empowered with the knowledge to stay at risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Holland Moor Primary School will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head Teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head Teacher for further CPD.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy.

Internet access – You must not access or attempt any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks.

Use of Email – Staff are not permitted to use school email addresses for personal business. All emails should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Password – Staff should keep passwords private. There is no occasions when a password needs to be shared with another member of staff or student, or ICT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pen drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT – You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head Teacher who will set the boundaries of personal use.

Images and Videos – You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT – use of personal ICT equipment is at the discretion of the Head Teacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware – any virus outbreaks are to be reported to the One Connect Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

Holland Moor Primary School

Bringing Out The Best

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidently damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let me teacher know if anybody asks me for personal information.

I will – let my teacher if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Holland Moor Primary School

Bringing Out The Best

Sample Letters to Parents:

Dear Parent/Carer

Use of Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorises websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact " head@hollandmoor.lancs.sch.uk "

Yours Sincerely

M Beale

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian –

Name of Child –

Signature - Date

E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Holland Moor Primary School	This policy was last reviewed in August 2019. *M Beale*