



INTERNET ACCESS POLICY – INCLUDING E-SAFETY

Version Date:	July 2018
Authors:	SLT
Review Date:	Annually

School Aims and Implementation

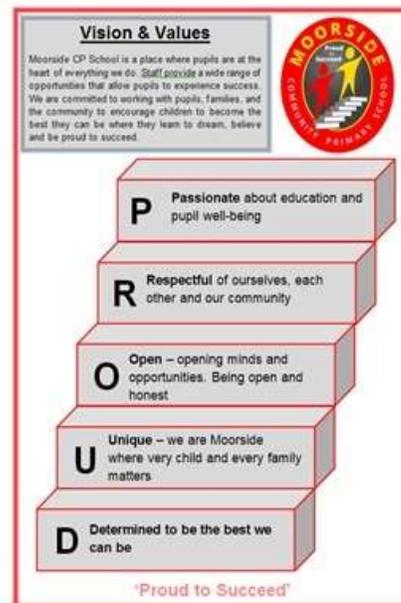
It is the primary aim of our school that every member of the school community feels valued, respected and that each person is treated fairly. We are a caring community, whose values are built on mutual respect for all in line with our equality policy.

Moorside Community Primary School aims to provide children the opportunity to develop towards their full potential; academically, emotionally and socially:

- Providing the highest standard of education to enable children to acquire the skills, knowledge and concepts relevant to their future.
- Promoting an ethos of care, mutual respect and support, where effort is valued and success celebrated.
- Enabling children to become active, responsible and caring members of the school and wider community.

The school works towards these aims by:

- Promoting high quality learning and attainment.
- Providing a high quality learning entitlement and environment.
- Valuing each other and ourselves.
- Working in partnership with parents and the community.



Introduction

Moorside Community Primary School believes that all children and staff should have access to our network and the Internet. Resources used for educational purposes in school are carefully chosen by teachers and determined by curriculum policies. However, the use of the Internet, by its nature, will provide access to information which has not always been selected by the teacher. Whilst pupils are often directed to sites which provide reviewed and evaluated resources, at times they will be able to move beyond these, to sites unfamiliar to the teacher.

The problems and issues that are highlighted by Internet use concerns all schools. There is cause for concern that children may access unsuitable material, either accidentally or deliberately.

The purpose of this policy is to:

- establish the ground rules that we have in school for using the Internet;
- describe how these ground rules fit into the wider context of our positive behaviour management systems and PSHE policies;
- demonstrate the methods used to protect pupils from websites containing unsuitable material.

At Moorside Community Primary School we feel the benefits that pupils receive from access to the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using the Internet lies with the classroom teacher. We believe that a combination of site filtering, close supervision and fostering a responsible attitude in our pupils, in partnership with parents, will ensure children's safety when using these resources.

Roles and responsibilities

E-Safety co-ordinator

Our e-safety co-ordinator is the person responsible for e-safety issues and has a leading role in establishing and reviewing the schools e-safety policy/ documents.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
- Provides training and advice for staff
- Liaises with school computing technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reports regularly to the Senior Leadership Team.
- Receives appropriate training and support to fulfil their role effectively.

The Headteacher

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety co-ordinator.
- The Headteacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Governors

- The governors are responsible for ensuring that the school is making every effort to safeguard children when implementing this policy. This will be carried out through receiving regular information about e-safety incidents and monitoring reports.

Classroom based staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school's Acceptable Use Policy for staff.
- They have reported any suspected misuse or problem to the E-safety Co-ordinator
- Digital communications with students (email/VLE/Voice) should be on a professional level and only carried out using official school systems.
- That e –safety awareness is embedded into the curriculum and other school activities.

The IT technician

The IT technician is responsible for ensuring that:

- The schools computing infrastructure is secure and not open to misuse or malicious attack.
- Users may only access the school's network through a properly enforced password protection policy.
- Shortcomings in the infrastructure are reported to the computing co-ordinator or the head teacher so that appropriate action may be taken.
- Has responsibility for blocking/unblocking internet sites in the schools filtering system. Passing on requests for blocking/unblocking to the computing helpdesk

Using the Internet for Education

The benefits include:

- access to a wide variety of educational resources including art galleries, educational websites, libraries and museums;
- rapid and cost effective world-wide communication;
- gaining an understanding of people and cultures around the World;
- staff professional development through access to new curriculum materials, experts' knowledge and practice;
- keeping abreast of news and current events;
- ability to take part in live discussions with experts;
- access to a range of multimedia resources to support work across the curriculum.

Pupils are taught about the vast information resources available on the Internet and the opportunity for their use is regularly planned into lessons across the curriculum. Teaching staff will review and evaluate websites intended for use in their lessons and will aim to select appropriate websites for their pupils' age range and ability.

Pupils will have the opportunity to exchange information via email. They will be taught how to use the features of email programs safely at all times.

Pupils will also be taught how to use searching techniques to locate specific information. We aim to ensure that children learn to make decisions about appropriate Internet use.

At times, information such as photographs, text or video clips may be downloaded for use in pupils' presentations and independent work.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow schools policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment: the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/ video images that pupils are appropriately dressed and are not participating in activities that may bring the individuals or the school into disrepute,
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Pupils Access to the Internet

As part of our commitment to e-safety we recognise that it is our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets.

Moorside Community Primary School uses EXAnet which includes a firewall service that minimises the chances of pupils encountering unsuitable material.

Pupils will only be permitted to use the Internet during lessons and organised before and after-school clubs.

Members of staff are aware of the potential for misuse and are responsible for explaining our expectations to pupils.

The computing subject leader will have access to pupils' email and other Internet related files and will put in place a timetable to check these to ensure that expectations of behaviour are being met.

Expectations for Pupils Using the Internet

Pupils who use the Internet in school all have written permission from their parents to do so – *the rules that children and parents have agreed to include:*

- *I will ask permission before using the Internet or Email and will have a clear idea of why I am using it;*
- *I will not interfere with, or knowingly change any settings on the computers;*
- *I will not install or delete any software on the computers;*
- *I will not change or create any passwords or login procedures without permission;*
- *I will not access or change other peoples' work files;*
- *I will only use school computers for school work or homework, unless I have permission for other uses;*
- *I will report to an adult any unsuitable material or messages sent to me or discovered by me;*
- *I understand that school may check my computer files and may look at any Internet sites I visit;*

- *I will not give my home address, telephone number or full name to anyone over the Internet;*
- *I understand that if I do not follow the rules, I will not be allowed to use the Internet, Email or any of the school's computers.*

Pupils are responsible for appropriate behaviour on the school's computer network, just as they are in the classroom or on the school playground. General school rules and our Behaviour Policy apply and it is expected that all users comply with the guidelines of this policy.

Expectations for Staff Using the Internet

Moorside Community Primary School has adopted the Calderdale Council Policy on Internet and Email use. **See Appendix 1**

E-Safety Education

- All members of the teaching staff at Moorside Community Primary School have been trained on the subject of e-safety through staff training days and parents have received information regarding keeping children safe on the internet through class letters, leaflets, informal meetings and via the school website.
- All pupils in school are taught to use the internet safely and responsibly during PSHE and computing lessons.
- A planned e-safety programme is also provided as part of the 'Rising Stars' Computing programme.
- Before any internet based unit of work, the class teacher is responsible for ensuring that their class understand the safety rules involved.
- Where pupils are allowed to freely search the internet e.g. using search engines, staff should be vigilant in monitoring the content of the website the young people visit.

The School Website

Moorside Community Primary School currently has a web page

The website may be used to celebrate achievements, promote the school and publish materials and resources for homework.

- no names that identify individual children will appear on our website;
- children's home information and personal email identities will not be included on our website. We will only include a point of contact for the school, such as the school phone number, office email and address;
- group photos will not include name lists;
- we will have signed parental consent to use photographs of all children who appear on our website;
- we will not display photographs of pupils who are no longer included on our roll;
- work displayed will be of the highest quality and reflect the status of the school.

Cyber-bullying

The term cyber-bullying is used to describe the use of technology such as text messaging, instant messaging, social networking websites (Facebook, Bebo), digital video and photography, internet chat rooms and Email for the purpose of bullying. At Moorside Community Primary School, we take reports of cyber-bullying very seriously and deal with and record incidents as we would for any other bullying case. Please see our behaviour policy for further information.

Appendix 1

POLICY ON INTERNET AND E-MAIL USAGE

The Internet is an unregulated environment. Although the MCPS has implemented pro-active filtering the School will not be liable for any material viewed or downloaded.

This Policy is neither exclusive nor exhaustive; if you are in any doubt about whether you should be using the facilities for a particular purpose – consult the Headteacher.

The school's internet and email facilities remain the school's property at all times, and the school may intercept communications for the purpose of monitoring or for keeping a record of communications relevant to the school's business. Where misuse of these facilities is suspected, detailed investigations will be undertaken. Failure to comply with this Policy may constitute gross misconduct and could lead to dismissal. Suspected illegal activities may also be reported to the Police.



RED – Unacceptable Use

- DO NOT knowingly, view, send or receive material, which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- DO NOT use the Internet and e-mail facilities for personal purposes in works time, UNLESS usage is in compliance with the Green – Acceptable Use section below.
- DO NOT use e-mail to engage in gossip.
- DO NOT make libellous statements about individuals or other organisations.
- DO NOT make statements purporting to represent the school when they are personal views.
- DO NOT make derogatory remarks or express derogatory opinions regarding the school.
- DO NOT knowingly, infringe copyright or intellectual property rights.
- DO NOT knowingly, use the facilities for any activity, which is illegal or fraudulent.
- DO NOT use the facility to pursue personal business interests, for gambling or for political purposes not directly related to your job.
- DO NOT allow anyone else to use your Internet access or e-mail account or provide any other person with the means to access these facilities e.g. By disclosing your user ID and password etc.
- DO NOT knowingly, engage in any activity, which threatens the integrity or availability of the school's systems.
- DO NOT attempt to gain unauthorised access to (hack) any server/facility whether inside or outside the school
- DO NOT Install any unauthorised programs, such as screen savers, on the school's information assets.



GREEN – Acceptable Use

- YOU MAY use the Internet and e-mail facilities for work purposes.
- YOU MAY use the Internet and e-mail facilities for personal purposes outside works time.
- YOU MAY open personal e-mails received in your school e-mail account in works time.
- YOU MAY use the facilities, with the prior approval of your manager, for personal purposes in works time.