Primary eSafety Framework Document

Scorton and Calder Vale CE Primary Schools

Developing and Reviewing this Policy

This eSafety Policy has been written as part of a consultation process involving the following people:

Sarah Thwaites, Helen Hesketh School staff at both establishments

The Governing Body of both schools

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy

Amended - Date: June 2015

Accepted – date November 2015

The implementation of this policy will be monitored by: **Sarah Thwaites and Helen Hesketh**

This policy will be reviewed as every 2 years.

Contents

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection

2. Your school's vision for eSafety

At both Scorton and Calder Vale Primary Schools, we value the contribution that Computing can make for the benefit for all members of the school community. To this end the school uses different areas of computing to motivate and include all pupils. All staff believe that effective use of computing technologies can enhance, enrich and extend learning and teaching across the curriculum.

Our vision encompasses the following aims:

- To enable all members of the school community to use computing technologies confidently in different situations
- To provide the children with the necessary skills that they can transfer into real life situations
- To enable all children to become independent learners
- To enable all children to use the Internet in a safe environment and to be critical and discerning with information found
- To promote and to use Computing to extend and develop communication skills
- To prepare all for the challenging world of changing technology

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

How does the Internet benefit education?

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the DfES Computing in Schools ;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LEA and DfES.
- mentoring of pupils and provide peer support for them and teachers

How will Internet use enhance learning?

- The school Internet access is designed expressly for pupil and staff 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 Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3. The role of the school's eSafety Champion

Our eSafety Champion is Mrs Thwaites

The role of the eSafety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring an eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, staff, children and governors are updated as necessary.
- Liaising closely with the school's Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and practices

This eSafety policy should be read in conjunction with the following other related policies and documents:

- Anti-bullying
- Child protection
- Staff induction documents

4.1 Security and data management

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The *Lancashire ICT Security Framework* (published 2005) should be consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

All data in your school must be kept secure and staff informed of what they can or can't do with data through the eSafety Policy and statements in the Acceptable Use Policy (AUP).

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- All staff are aware that some mobile devices e.g. mobile phones, game consoles or net books may access unfiltered internet content.
- All mobile devices used in school will be the property of the school.
- Children are not allowed to bring mobile devices (including phones) into school.
- Staff are expected to leave personal mobile devices outside the classroom
- If an instance should arise where there may be an educational benefit to extended learning through the use of a child's personal mobile device, the class teacher must seek permission from the Computing coordinator before it is used. It would also have to be virus checked.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- School seeks consent from the parent/carer or member of staff who appears in the media or whose name is used.
- Parental/carer permission obtained.
- School may retain images of pupils after they have left the establishment, but will not use them again for a different purpose without further permission being sought.
- Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- Parents/carers, who have been invited to attend school events, will be allowed to take videos and photographs and will be made aware of any conditions (only for personal use with no sharing on public forums) in advance. This will be done through ticketing, regular reminders on the weekly news letter and verbal reminders before key events or performances.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.

- School ensures that photographs/videos are only taken using school equipment and only for school purposes.
- School ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff are only allowed to store digital content on school equipment with a full understanding of their responsibility for the confidentiality and acceptable use of such material.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy, will be constantly monitored by the ICT team with vigilance displayed by all school staff.

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated
risks.

Email

In our school the following statements reflect our practice in the use of email.

- All users have access to the Lancashire Grid for Learning service as the preferred school email system.
- Only official email addresses are used between staff and with pupils/parents when personal/sensitive data is involved. Staff also have access to secure mail service hosted by Lancashire Grid for Learning where confidential or sensitive information is being shared.
- The Lancashire Grid for Learning filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Bebo and Club Penguin. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.
All staff need to be aware of the following points:

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils must not be added as 'friends' on any Social Network site.
- Children who are under 13 are not legally allowed to members of Facebook.

Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- The school allows personal mobile phones to be used in school by staff and visitors but are asked to be left on silent in curriculum time.

- It is acceptable to use personal mobile phones for school activities e.g. school trips for the purposes of maintaining contact with the base but not for taking pictures.
- It is not acceptable to use personal mobile phones to support lessons.

Instant Messaging:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

- All instant messaging is to be conducted in the presence of a teacher who is aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts. This communication can only be done using school equipment.

Virtual Learning Environment (VLE) / Learning Platform:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

At present the school has chosen not to use the VLE.

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- E-Safety messages will be communicated to parents/carers on both the school website and the 'Bowland Blogger'.
- Everybody who has access to edit the web site and blog is made aware of the guidance for the use of digital media on web based publications.
- Everybody who has access to edit the web site and blog is made aware of the guidance regarding personal information on web based publications.
- The Headteacher has overall responsibility for what appears on the website and blog.
- Information on the school website and blog is available for everybody to see.

Video conferencing:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- A permissions letter must be made available for parents/carers to sign giving permission for their child/children to participate in video and

photographs. Children will not be appearing 'live' on the Internet through a video conferencing link.
However, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.

- Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to „stop" or „hang up" the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.
- Recordings are not to be repurposed in any other form or media other than the purpose agreed.

Ipads /Netbooks

The policies, procedures and information applies to all iPads, iPod Touches or any other IT handheld device used in school.

User Responsibilities

- The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc) on top of the iPad.
- Users must use protective cases/covers when using the iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extremes of temperature.
- Do not store or leave unattended in vehicles.
- Ensure all Ipads are returned to the trolley to ensure syncing and charging takes place.

Safeguarding and Maintaining as an Academic Tool

- Users may not photograph any other person without that person's consent
- Photographs of children must be in line with Consent Letter Agreement
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad as safe and secure as possible.

Prohibited Uses

- Images of other people may only be made with the permission of the person, or parents of the person, in the photograph.

- The iPad is a school tool designed to enhance classroom practice. It is not for personal use e.g. Facebook or social networking sites and should stay in school unless permission is given by the IT/Computing Co-Ordinator or Head Teacher.

Lost, Damaged or Stolen iPad

- If the iPad is lost, stolen or damaged, the ICT Co-Ordinator or Head Teacher must be informed immediate

Others:
The School will adapt/update the eSafety policy in light of emerging new technologies and any issues or risks associated with these technologies.

4.5 Acceptable Use Policy (AUP)

Use of ICT for educational, personal and recreational purposes.
AUPs (see appendix 2,3,4 & 5) are used for Staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.

Our school AUP aims to:

- Be understood by the each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the eSafety

Policy/AUP.

- Outline acceptable and unacceptable behaviour when using technologies, for example:
- Cyberbullying

- Inappropriate use of email, communication technologies and Social Network sites and any online content.
- Acceptable behaviour when using school equipment /accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of eSafety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

4.6 Dealing with incidents

Here are the types of incident that may occur and how these will be dealt with in our school.
An incident log will need to be completed to record and monitor offences (see appendix 1) . This will be audited on a regular basis by the Computing Subject Leader or other designated member of the Senior Leadership Team.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the
Headteacher who must refer this to external authorities, e.g. Police, LCC Safeguarding,CEOP,
Internet Watch Foundation (IWF). **No staff member will ever personally investigate, interfere with or share evidence as they may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident-

Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) .They are licensed to investigate – schools are not!
Examples of illegal offences are:
Accessing child sexual abuse images
Accessing non-photographic child sexual abuse images

Accessing criminally obscene adult content
Incitement to racial hatred
More details regarding these categories can be found on the IWF website http://www.iwf.org.uk

Inappropriate use

It is more likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Examples of inappropriate incidents are listed below with suggested sanctions for our school.

Incident	**Procedures and Sanctions**
Accidental access to inappropriate materials	Minimise the webpage/turn the monitor off. Tell a trusted adult. Enter the details in the Incident Log and report to LGfL filtering services if necessary. Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	Using other people's logins and passwords maliciously. Inform SLT or designated e-Safety Champion. Enter the details in the Incident Log. Additional awareness raising of Deliberate searching for inappropriate materials.
Bringing inappropriate electronic files from home.	e-Safety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement, for specific or repeated non-accidental incidents.

Procedures when dealing with E-Safety;

- Responsible persons – Headteacher, E-Safety Champion.
- All staff made aware of our procedures to recognise and deal with E-safety incidents (see appendix 9)
- Responding to safety incidents will be displayed in Staffroom and ICT Suite as a guidance
- Children are given e-safety guidance as part of curriculum each term
- Incidents will be logged on Form Appendix 1 in file in ICT Suite and monitored by E-Safety Champion
- Review of policy/procedures in line with frequency and seriousness of incidents.

5. Infrastructure and technology

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are provided (by default) by the Lancashire Grid for Learning.

Pupil Access:

- Pupils will only have supervised access to the internet. No access will be allowed during playtime or lunch time. Pupils only be allowed access when a positive consent form has been returned. An upto-date list is available from the school office.

Passwords:

- Children only have class access. Teachers have class and staff access. The administrator password is known by the IT technician, Headteacher and Teaching Staff.

Software/hardware:

- The school has legal ownership of all software.
- The school has an up to date record of appropriate licences for all software and the IT co-ordinator is responsible for maintaining this.

Managing the network and technical support:

The network is managed and technical support provided by EdIT solutions.

- Servers are located in a secure cupboard where there is no pupil access.
- All wireless devices have had their security enabled.
- The technician responsible for managing the security of the curriculum school network and the Westfield Centre manage the security of the office network.
- Computers are regularly updated with critical software updates/patches by the technician.
- Breaches of security must be reported immediately to the Headteacher or ICT subject leader.
- Laptops may be used for personal use but must not be used by family members.
- Technical support providers are made aware of our schools requirements / standards regarding eSafety.
- It is the IT/Computing subject leader's responsibility to liaise with/manage the technical support staff.

Filtering and virus protection:

- Filtering may be performed by the ISP, by the LEA, at school-level or by any combination.
- The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Staff and pupils will only use the Google search engine as this is filtered by the County Council.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT subject leader.

- Staff are expected to bring their laptops into school on a regular basis to have security software updated.

- Suspected or actual computer virus infection should be reported immediately to the ICT subject leader or technician.

6. Education and Training

In 21st Century society, pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

Area of Risk	Examples of Risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Virus', Trojans, Spyware Premium Rate services Online gambling.
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Pupils need to be taught that not all content is appropriate or from a reliable source. Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr,

	Cyber-tattoo, Sexting.
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact.

6.1 eSafety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own eSafety. Both Scorton and Calder Vale Schools provides suitable eSafety education to all pupils:

- Regular, planned eSafety teaching within a range of curriculum areas (using the Lancashire ICT Progression framework)
- E-Safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- The school ensures that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of IT both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, eSafety rules (See Appendices).

6.2 eSafety – Raising staff awareness

- All staff must accept the terms of the Acceptable Use Policy before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the eSafety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Regular training will be organised by the eSafety champion for all staff.

6.3eSafety – Raising parents/carers awareness

'Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.' (Byron Report, 2008).

- The school offers external information sessions by CLEOP approved trainers for parents.
- Further information for parents is available on the school website.
- Information on eSafety is included in newsletters to parents.

The school offers opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies. For example through:

- School newsletters, Website and other publications.
- Promotion of external eSafety resources/online materials.

6.4eSafety – Raising Governors' awareness

The school considers how Governors, particularly those with specific responsibilities for eSafety, ICT or child protection, are kept up to date. This is through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

NB The eSafety Policy will be reviewed yearly (and/or if a serious breach occurs) by the eSafety coordinator, approved by the governing body and made available on the school's website.

7 Standards and inspection

The eSafety policy will be reviewed annually and will incorporate new technologies.

- A risk assessment will be carried out before any new technology is incorporated into teaching and learning. These risk assessments will be incorporated into the policy. ??

- ESafety incidents will be monitored and recorded by the headteacher. These will be analysed to see if there is a recurring pattern.

- Patterns of eSafety issues will be addressed thorough assemblies, workshops and class discussion activities where appropriate.

- Changes to the eSafety policy will be discussed at staff meetings and staff will disseminate this information to pupils in an age-appropriate way.

- The eSafety policy will be reviewed by the curriculum sub-committee of the governing body and will be made available to parents.

- AUPs will be reviewed annually in the light of emerging technologies.

Appendix 1

Scorton and Calder Vale eSafety Incident log

All eSafety incidents must be recorded by School eSafety Champion or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Govenors.

Date/Time	Type of incident	Name of pupil(s) and staff involved	System details	Incident details	Resukting actions taken and by whom (and signed)
1 Jan 2014 *9.50am*	*Accessing inappropriate website*	*A N Other (pupils)* *A N Staff (class teacher)*	*Laptop 1 or ipad 1*	*Pupils observed by Class Teacher deliberately attempting to access adult websites*	*Pupil referred to headteacher and given warning in line with sanctions policy 1st stime infringement of AUP. Site reorted to LGFL.* *Esafety champion also informed.*

Appendix 2

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in
our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing eSafety as part of your child's learning, we will also be holding Parental eSafety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed.

In the meantime, if you would like to find out more about eSafety for parents and carers, please visit either the esaftey page on either schools website or the Lancsngfl eSafety website http://www.lancsngfl.ac.uk/esafety.

If you have any concerns or would like to discuss any aspect of the use of IT in school, please contact *Mrs Thwaites*

Yours sincerely,

Mrs Hesketh
Head Teacher

Appendix 3

Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

.....**Parent/ Carer Signature**

We have discussed this Acceptable Use Policy and..... [Print child's name] agrees to follow the eSafety rules and to support the safe use of IT at *Scorton and Calder Vale Primary School*

.

Parent /Carer Name (Print) .....

Parent /Carer (Signature) ....

Class ..... Date.....

Appendix 4

Acceptable Use Policy for ipads/netbooks (AUP) - Children and Staff

1. I will take good care of any iPad I use.
2. I will never leave any iPad I use unattended.
3. I will know where the iPad is at all times during my usage of it.
4. I will keep food and drinks away from the iPad since they may cause damage to the device.
5. I will protect the iPad by only carrying it whilst it is in a case.
6. I will use the iPad in ways that are appropriate.
7. I understand that the iPads are subject to inspection at any time without notice.
8. I will only photograph people with their permission.
9. I will only use the camera or the microphone when my teacher tells me to.
10. I will never share any images or movies of people in a public space on the Internet, unless I am asked to do so by my Teacher.
11. I will not hide any iPad so others cannot use it.
12. I agree to abide by the statements of this iPad acceptable use policy

I have read, understand and agree to abide by the terms of the iPad Acceptable Use Policy.

Name _____

Signature _____

Date _____

This AUP must be signed and returned before any access to school systems is allowed.

Appendix 5

ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of Kevin Egan/John Kavanagh.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .....

Date .....

Full Name .....(PRINT)

Position/Role .....

Appendix 6

Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests.

To be signed by any adult working in the school for a short period of time.
1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or
relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile
phone, at all times.
7. I understand that network activities and online communications are monitored, including any
personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not
followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.
Signature
.....
Date
.....
.....
Full Name
.....(PRINT)
Position/Role
.....

Appendix 7

Our Golden Rules for Staying Safe when using computers

- We only use the Internet when a trusted adult is with us.
- We are always polite and friendly when using online tools.
- We always make careful choices when we use the Internet.
- We always ask a trusted adult if we need help using the Internet.
- We always tell a trusted adult if we find something that upsets us.

Appendix 8

Our Golden Rules for Staying Safe when using computers

- We always ask permission before using the internet.
- We only use the Internet when a trusted adult is around.
- We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).
- We always tell an adult if we see anything we are uncomfortable with.
- We only communicate online with people a trusted adult has
- approved.
- All our online communications are polite and friendly.
- We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.
- We only use programmes and content which have been installed