Downholland Haskayne CE Primary School

E-Safety Policy

The Governing Body of Downholland Haskayne CE Primary School have adopted this policy which will be reviewed on an annual basis.

Signed **Mrs N Hains** **Head Teacher**	**Signed** **Rev Paul Robinson** **On behalf of the Governing Body**
Nicky Hains **Print Name**	**Paul Robinson** **Print Name**
Date: November 2019	**Proposed Review Date: November 2020**

E-Safety Policy 2019

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

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

Our e-Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

Our vision for e-Safety

The Internet is an essential element of 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 statutory curriculum and a necessary tool for staff and pupils.
The benefits include:

- Access to a wide variety of educational resources including libraries, art galleries 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
- Exchange of curriculum and administration data with LA/DCSF
- Social and leisure use
- Greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others**.**

At Downholland Haskayne CE Primary School, we feel that the best recipe for success lies in a combination of site filtering, supervision and by fostering a responsible attitude in our pupils in partnership with parents.

The role of the school's e-Safety Champion

The e-Safety Champion is the point of contact for e-safety issues and incidents, however certain responsibilities may need to be delegated to other staff e.g. Designated Senior Person/Child Protection Officer as appropriate.

The role of the e-Safety Champion includes:

- Operational responsibility for ensuring the development, maintenance and review of the School's e-Safety 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 e-Safety incident occur.
- Ensuring the e-Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with e-Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging e-Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head teacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

Policies and practices

This e-Safety policy should be read in conjunction with other related policies and documents, including School Self Evaluation Framework, School Improvement Plan, Staff Code of Conduct, Recruitment and Induction Procedures, Anti Bullying Policy, Behaviour Policy, Child Protection Policy, Lancashire County Council ICT Security Framework for Schools.

Security and data management

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

All staff are aware of the need to ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately, whether in school, taken off the school premises or accessed remotely. If it is necessary for a member of staff to save personal data onto their home information system, they will consult with the Head teacher or ICT Co-coordinator. See appendix 1 Staff and governors Acceptable Use Agreement.

Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. Staff and other adults working in school are aware that some mobile devices can access unfiltered internet access and care should be taken accordingly.

Use of digital media

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed, for example video conferencing.

All images of children or staff must be taken on the school cameras only. These images must be downloaded onto the Office computer and will be deleted when necessary, unless agreed by the Head Teacher.

In our school we are aware of the issues surrounding the use of digital media online. At times, information such as text, photographs may be 'downloaded' from the internet for use in pupil's presentations. As part of our e-safety training staff and pupils will be made aware of the copyright laws. Text and images will be checked and monitored by staff.

As photographs and video of pupils and staff are regarded as personal data in terms of the Data Protection Act (1998), school must have written permission for their use from the individual and/or their parents or carers.

Communication technologies

The school will provide access to the telephone, email and the internet for all staff for work related purposes. Staff are permitted occasional personal use of the telephone, email and the internet, outside their timetabled working hours. The school will not make a charge for this, provided the privilege is not abused. All digital communications should be professional in tone and content.

Email

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

- 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.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to BT Lancashire Services .
- 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.

- We include a standard disclaimer at the bottom of all outgoing emails

Example school e-mail disclaimer:

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Lathom Park CE School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Web sites and other online publications

This may include for example, pod casts, videos, 'Making the News' and blogs.

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The Head teacher will approve any new pages for the web site before they go on-line. This will be as printed copies of the page, or pages on the web site, hidden until approved to be online.

Photographs of children **will not** be used on the web site. Pupils' full names will not be used anywhere on the Web site. See appendix 4 Image consent form and appendix 4a image consent – conditions of use

Social Networks:

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter and Club Penguin. These sites provide users with simple tools to create a profile 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. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old.

These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

All staff must be aware of the following points:

- That they familiarise themselves with the sites 'privacy settings' in order to ensure the information is not automatic
- That they do not conduct or portray themselves in a manner which may:-
    - ✓ Bring the school into disrepute
    - ✓ Lead to valid parental complaints
    - ✓ Be deemed derogatory towards the school and or/employees

- ✓ Be deemed derogatory towards pupils and/or parents and carers
- ✓ Bring into question their appropriateness to work with children and young people

- 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 as private.
- Pupils must not be added as 'friends' on any Social Network site.

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:

Generally staff's personal mobile phones should not be used in the school setting except for emergencies. The use of a mobile phone must not detract from the quality of supervision and care of the children. However, staff may use their personal mobile phones as a means of contact during school trips and out of school activities.

Children are allowed to bring mobile telephones to school for emergency contact use only. These must be given to their class teacher or taken to the office for safe keeping. Children will not be allowed to use a mobile phone for any other purpose e.g. taking photographs.

Instant Messaging

Instant Messaging, e.g. MSN, Skype, Yahoo Messenger, is a popular communication tool with both adults and children. It provides an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' these sites by default, but access permissions can be changed at the request of the Head teacher.

Video conferencing:

Before a video conferencing event, approval by the Head teacher will be obtained in advance. All sessions should be logged including the date, time and the name of the external organisation/person(s) taking part. Parents/carers will be asked 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.

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.

Others

The school will adapt update the policy in the light of emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication as necessary.

Acceptable Use Policy (AUP)

An Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. AUPs are recommended for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. You may wish to consider this agreement 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 must be kept in school and made available to all staff. See appendices

1. Staff and Governor acceptable use ICT agreement
2. Supply Teachers and visitors/guests ICT acceptable use agreement
3. School, Pupil, Parent Internet ICT acceptable use agreement

Dealing with incidents

An incident log will be completed to record and monitor offences. This will be audited on a regular basis by the e-Safety Champion or Head teacher.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP and Internet Watch Foundation (IWF).

Please note: **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.**

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

Inappropriate use

It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

Incident	Procedure and sanctions
Accidental access to inappropriate materials	• Minimise the webpage or 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	• Inform e-Safety Champion. • Enter the details in the Incident Log. • Additional awareness raising of 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
Deliberate searching for inappropriate materials	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way	

CyberBullying

Many young people experience the internet and mobile phones as a positive, productive and creative part of their activities and development of their identities. Also information communication technologies support social activity that allows young people to feel connected to their peers.

Unfortunately, technologies are also being used negatively. When children are the target of bullying via mobile phones or the internet, they can feel alone and very misunderstood. They may not be able to identify that what is happening to them is a form of bullying, or be confident that the adults around them will understand it that way either.

CyberBullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. At St Mark's no type of bullying is acceptable. The school will provide key safety advice for the children, staff and parent about CyberBullying. See CyberBullying A Whole School Issue (DCSF-00685-2007) and any incidents will be dealt with in line with the School's Anti-Bullying policy

Infrastructure and technology

Downholland Haskayne School will ensure that the infrastructure/network is as safe and secure as possible. We subscribe to the Lancashire Grid for Learning/CLEO Broadband Service, internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service.

Sophos Anti-Virus software is included in the school's subscription, and is installed on computers in school and configured to receive regular updates.

Pupil Access

The children will only use the internet when there is a responsible adult present to supervise.
However it is unrealistic to suppose that the teacher's attention will always be directed towards the computer screen. Every possible precaution will be made by staff to ensure appropriate use of the internet by children.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through the SMART rules. See **Education and Training** and Appendix 5 SMART

Rules

Passwords

All users of the school network have a secure username and password. There is a generic password for Reception to enable them to access software and internet activities and tasks. The administrator password for the school network is available to the Head teacher and it is kept in a secure place. Staff and pupils are reminded of the importance of keeping passwords secure as part of the e-safety curriculum.

Software/hardware

All software is licensed and copies of licences are kept in the office. Software can only be loaded by ICT technician at the request of the Head teacher or ICT co-ordinator. Regularly updated software toolkits and Hardware audits are available to staff and software. See Schools ICT policy.

Managing the network and technical support

The server and cabling are securely located in the Coms box in the stock room. An ICT technician from BT Lancashire Services (Lancashire ICT Centre) is responsible for keeping the security of the network up to date with critical software updates.

Users have clearly defined access rights; pupils can access their documents and the pupil's folder. Teachers can access their documents, pupils' folder and the teacher's folder; they may also download/load additional software with permission of the Head teacher or ICT co-ordinator.

All staff and pupils are required to log out when they leave a computer unattended. All users must report any suspicion or evidence of a breach of security to the ICT co-ordinator or the Head teacher.

Staff are permitted to use USB pens to store or transfer data, but these must be regularly checked for viruses and staff are aware that information stored on the pen can be monitored by the ICT coordinator or Head teacher.

Staff issued with school lap tops will be required to sign a Laptop for teachers and staff agreement.

Filtering and virus protection
At our school we subscribe to the Lancashire Grid for Learning/CLEO Broadband Service, internet content filtering. Staff are aware of the procedures for blocking and unblocking specific website. All computers, including laptops are regularly updated with the most recent version of virus protection software.

Education and Training
In 21st Century society, staff and 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.

Safety across the curriculum
It is vital that pupils are taught how to take a responsible approach to their own e-Safety. There are three main areas of e-Safety risk.

Areas 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.	• Illegal materials • Inaccurate/biased materials • Inappropriate materials • Copyright and plagiarism • User-generated content e.g. You Tube, 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 • Cyber bullying • Contact Inappropriate (emails/instant messaging/blogging) • Encouraging inappropriate contact

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet through the SMART rules. See E-safety rules will be posted in all networked rooms (ICT suite and classrooms) and discussed with the pupils at the start of

each year and will be reminded regularly, particularly when the children are using the internet.

Pupils will be made aware of what is appropriate and inappropriate use of the computer and the implications for inappropriate use. See **inappropriate use** and will be asked to sign a Pupil Acceptable Use agreement. The children will be recap on this agreement at the beginning of each school year. Pupils will be informed that network and Internet use will be monitored.

There will be a designated e-safety day each year, with follow-up session for parents as appropriate.

Raising staff awareness
All staff are expected to promote and model responsible use of ICT and digital resources. E-Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's e-Safety Policy and Acceptable Use agreement. The School e-Safety Policy will be available to all staff and its importance explained. All existing staff, governors, regular visitors and supply staff will be asked to sign an ICT Acceptable Use Agreement.

E- safety is discussed regularly at curriculum meetings and on the agenda for support staff and welfare meetings. Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

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).

Parents' attention will be drawn to the School's e-Safety Policy in newsletters, the school brochure and on the school Web site, for example access to the SMART rules, link to internet safety web site. There will also be e-safety follow up session linked to the school's annual e-safety day.

Parents will be asked to sign the pupil's ICT acceptable use agreement and read and sign image consent and conditions of use form.

Raising Governors' awareness
The e-champion will liaise with the specific governors with responsibilities for e-Safety, including ICT or child protection governors to ensure they are kept up to date.

NB: The e-Safety Policy should be regularly reviewed and approved by the Governing body.

Standards and inspection
Ensuring robust safeguarding procedure is a main priority at Downholland Haskayne School. The policy is reviewed annually and all staff and governors are kept up to date and any

changes or updates are added to the agenda of the next meeting e.g. Staff meeting, governors curriculum committee meeting.

Any e-safety incidents completed in the log. See appendix 6 Incident log. The log will be will be audited on a regular basis by the e-Safety Champion/ICT co-ordinator or Head teacher.

As part of the e-Safety day the children will complete an e-safety questionnaire which will be analysed to ensure e-safety education is contributing to safer ICT and internet practices.

The policy and appendices, including the acceptable use agreements will be reviewed at least annually and will include reference to new trends and emerging technologies.