CARR HILL COMMUNITY PRIMARY SCHOOL

E-SAFETY POLICY

RATIONALE

The potential that technology has to impact on the lives of all people increases every year. This is probably even truer for children who are generally much more open to developing technologies than adults. In many areas, technology is transforming the way schools teach and the way children learn. At home, technology is changing the way children live and the activities they choose to partake in. These trends are set to continue and while developing technology brings many opportunities, it also brings the following risks and potential dangers:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of and sharing of personal information and images.
- The risk of being subject to grooming by those they make contact with on the internet.
- Inappropriate communication or contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video and internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement, illegal down loading of music or video files.
- The potential for excessive use, which may impact on social and emotional development.

This policy sets out how we strive to keep children safe with technology while they are in school and sets out how we educate children of the potential risks when using technology at home. We also explain how we help those who work with our children beyond the school environment (parents/carers etc) to be aware and to assist in this process.

Breaches of an E-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that on line actions can have.

RESPONSIBILITIES

Our ICT Co-ordinator is responsible to the Headteacher and Governing Body for the day to day responsibility of E-Safety issues, including:

- Reviewing the school's E-Safety policy annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident.
- Providing training and advice for staff.
- Liaising with the Local Authority where necessary.
- Liaising with ICT Technical Support to ensure that internet access is appropriately filtered.
- Receipt of e-Safety incidents and maintaining a log of incidents to inform future e-Safety developments.
- Attendance at relevant meetings and committees of Governing Body when required.
- Reporting termly to the Headteacher so that E-Safety (which will include anonymous details of any incidents) can be reported to the Governing Body via the Headteacher's Report to Governors.

Governors are responsible for ensuring that this policy in reviewed and enforced effectively.

The Head Teacher 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 ICT Co-ordinator. The Headteacher and the Deputy Headteacher 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.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-Safety matter,participate in annual e-Safety training and have read the school e-Safety Policy.
- They have read, understood and signed the school's Acceptable Use Agreement for staff.
- They report any suspected misuse or problem to the e-Safety Co-ordinator.
- e-Safety issues are embedded in the curriculum and other school activities.

ACCEPTABLE USE

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate Acceptable Use Agreement AUG). AUGs are in place for staff, volunteers, children and parents/carers and set out the expectations when using school ICT equipment. As part of their induction, new staff are given the appropriate AUG and current AUGs are reviewed as needed in order to ensure that the policy within reflects the most recent developments in technology. The AUG is discussed with children as part of the e-Safety education and copies are sent home to enable parents/carers to discuss the expectations with their children and support the school in providing a safe learning environment.

ILLEGAL OR INAPPROPRIATE ACTIVITIES

The school believes that the activities listed below are inappropriate in a school context (the first 4 points are illegal) and users should not engage in these activities when using school equipment/systems, in or out of school. Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images (illegal - The Protection of Children Act 1978).
- Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal - Sexual Offences Act 2003).
- Possession of pornographic images (illegal - Criminal Justice and Immigration Act 2008).
- Criminally racist material in UK - to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal- Public Order Act 1986).
- Pornography.
- Promotion of any kind of discrimination, racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

The following activities are also considered unacceptable on the school's ICT equipment:

- Using school systems to run a private business.
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, down loading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer / network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained high volume network traffic (down loading / uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gambling and non-educational gaming.
- Use of personal social networking sites / profiles for non-educational purposes.

If members of staff suspect that misuse might have taken place, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible, through normal behaviour management procedures.

USE OF MOBILE PHONES/HAND HELD DEVICES

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Staff/Volunteers/Visitors are permitted to bring their mobile phones in to school but they MUST NOT be used in areas accessed by pupils or when supervising pupils. Staff can, however, request permission from the Headteacher to keep a phone switched on in certain circumstances (e.g. an expected and important phone call).
- Older pupils (Years 5 and 6) who walk home from school alone are permitted to bring mobile phones into school, with written agreement from parents,. All pupil phones are kept safe in the school office and collected by the children when they leave school.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Staff are not permitted to use their own personal phones or devices for contacting pupils or their families within or outside of school in a professional capacity. Where contact with pupils or parents/carers is required, staff must use the school phone.
- Staff/Volunteers/Visitors must not use personal devices such as mobile phones or cameras to take photos or videos of pupils and must only use work-provided equipment for this purpose (volunteers/visitors will never be required to take photos or videos of pupils).

E-MAIL

Email accounts are set up for all staff in school - Office 365 for Teaching and Support staff, Gateshead Council's Microsoft Outlook for Admin staff. These official school email services may be regarded as safe and secure and are monitored.

Pupils may only use e-mail accounts set up and approved by the school. When sending emails, pupils must not reveal personal details of themselves or others, or arrange to meet anyone without specific permission. E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

SCHOOL WEBSITE

Our school website is used to inform and share information with the community beyond our school, including celebrating work and achievements of children. All users are required to consider good practice when publishing content. Personal information should not be posted on the website. Pupils' work can only be published with theirs or their parent’s permission.

USE OF DIGITAL AND VIDEO IMAGES

There are important safety concerns to consider before placing photos of children on the school's website or twitter account. We have a duty of care for our children which, in the context of our website/twitter account, means we must ensure that no individual child can be identified or contacted either via, or as a result of a visitor using the website/twitter account.

Placing photos on line opens those in the photograph up to potential dangers such as from those wishing to exploit young people.

The DfE advises the following as a broad rule of thumb:

- If the child is named, avoid using their photograph.
- If the photograph is used, avoid naming the child.

Carr Hill's Governing Body have agreed the following:

- Parental permission must be obtained before publishing any photographs of children on line. The permission of the children should also be obtained. Permission is sought at the beginning of each academic year when the child's data is forwarded to parents for confirmation. If permission is not given by parent/carer then no photographs should be taken of that child.
- If you upload a photograph, do not use the child's name.
- If you use the child's name, do not upload a photograph. There should be no need to use the child's full name - forename and initial of surname should be sufficient for parent/carers to identify their child, eg Freddie M.
- Ensure the appropriateness of the photo - it is important to be careful about how the individuals in it are portrayed. For example, pictures of children swimming or doing gymnastics are inappropriate.
- Individual contact details for children should never be given out on a website and in no circumstances be displayed under a photo of the child.
- Images must only be captured using school equipment (personal equipment of staff, like mobile phones etc, MUST NOT be used for such purposes).
- If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected;
- Under no circumstances should staff share or upload pictures of pupils on line other than via the school website or school protected twitter account.

INTERNET ACCESS

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. Parents/Carers will be asked to sign and return a consent form allowing their child to access the internet while at school.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The E-Safety Coordinator will record all reported incidents and actions taken in the School E-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Safeguarding Lead will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage E-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has or is taking place then the school will contact the Local Authority Designated Safeguarding Officer / e-Safety Officer.

How will e-Safety complaints be handled?

- Complaints about internet misuse by staff or pupils will be dealt with under the school's complaints procedure.
- All e-Safety complaints/incidents will be recorded by the school, including any actions taken.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Local Authority Designated Safeguarding Officer to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

SECURITY / FILTERING

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or inappropriate in an educational context.

If staff or pupils discover an unsuitable site, it must be reported to the ICT Co-ordinator.

The Admin Network is secured to a Public Service Network specification as per government requirements and managed by Corporate ICT Services.

The Curriculum Network, however, cannot sensibly be secured to such levels, primarily for business reasons - the main ones being:

- Pupils of a young age cannot be expected to change a password routinely nor be expected to remember a complex password;
- Schools have almost universally rejected a requirement for employees to be forced to change passwords on a monthly cycle;
- Whilst the School ICT Support Team centrally manage all devices of the curriculum active directory, they cannot "see" any standalone devices;

The School lCT Support Team therefore adopt a best practice approach as follows:

- Physical security at the Dryden Centre where central servers are only accessible by authorised staff or authorised third parties;
- Acceptable use agreements in place for end users;
- Incident response - incidents are reported to the School ICT Support Team and the school via the "forensic software" which runs in the background of the curriculum network and are acted upon as required;
- Access control - all user access is limited to that which is required to perform their function. Each pupil is assigned a unique user account, however schools commonly operate shared password solutions for pupils;
- Gateway controls are managed by Corporate ICT Services and assured controls are in place between the Admin Network and the Curriculum Network;
- All firewalls are EAL4 compliant and managed by Corporate ICT Services only;
- Web Gateway is configured with anti-malware, IPS and file down load checking;
- Email Gateway is configured with anti-malware and configured to block specific file types, content analysis, SPAM blocking and checks for file type tampering;
- Malware protection - only authorised devices are permitted on the curriculum network and all of these devices are managed by the SchoollCT Support Team;

Pupils are made aware of the importance of filtering systems through the school's E-Safety Education Programme.

Staff and Governors are made aware of the filtering systems through training.

Parents are informed of the school's filtering policy through e-Safety awareness sessions. No filtering system can guarantee 100% protection against access to unsuitable sites. The Local Authority on behalf of the school will therefore monitor the activities of users on the internet.

E-SAFETY EDUCATION

Whilst regulation/technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-Safety is therefore an essential part of the school's computing provision. Children/Young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them. E-Safety education is provided in the following ways:

- A planned e-Safety programme is provided as part of ICT lessons and is regularly revisited - this covers both the use of ICT and new technologies in school and outside school.
- We use the resources on CEOP's Think U Know site as a basis for our E-Safety education.
- Key E-Safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT both within and outside school.
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

SEXTING

Sharing photos and videos online is part of daily life for many people, enabling them to share their experiences, connect with friends and record their lives. Photos and videos can be shared as text messages, email, posted on social media or increasingly via mobile messaging apps such as Snapchat, Whatsapp or Facebook Messenger.

Sexting is a significant issue for older teenagers and involves the sharing of indecent images of themselves with others. It may be the intention for the image to be shared only with one person, but invariably these pictures or videos are shared across the internet. Such images can be a part of the early stages of grooming, especially when the potential victim has only "met" the abuser online.

Although sexting is becoming a widespread phenomenon, it is illegal to send or be in possession of indecent images or videos of people under 18 (Protection of Children Act 1978 and Criminal Justice Act 1988).

Why do people send "sexts"?

- Experimental phase prior to being sexually active
- As a joke or a dare
- Fun or flirtatious
- In lieu of sexual activity
- To fit in
- Proud of their body
- To show commitment to a relationship
- Because they are "in love"
- Easy to do – anonymous

Why is "sexting" such a problem?

- It is illegal to send or possess images of under 18s
- Revenge or intimidation after a relationship comes to an end
- Lose control of where the images or videos go
- Lead to depression and suicide of victims
- An aspect of grooming for child sexual exploitation

Our approach to handling concerns relating to "sexting" is reflected in our *Child Protection/Safeguarding Policy* as required by the government's Keeping Children Safe in Education statutory guidance. In any event of "sexting" the school will liaise with parents/carers and other services where deemed to be appropriate.

SOCIAL NETWORKING SITES - TWITTER

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation.

Carr Hill's Governing Body have agreed that a controlled twitter account is appropriate for the needs of the school, parents/carers and pupils. This allows the school to inform parents/carers when necessary.

The Headteacher, via the School Business Manager and e-Safety Co-ordinator will control access to the school twitter account. Staff have been advised that only these members of staff can accept "follower requests" and when doing this will ensure that they turn off that follower's ability to "retweet tweets".

In terms of child safety and school liability of using Twitter, Carr Hill's account is a locked (non-public, non-searchable) account. This prevents people from following @CarrPrimary automatically - once they ask to follow @CarrPrimary, an email is sent to the school's email account so we can verify if the follower is a family member. In effect, this means that we are "vetting" users. It also means that our tweets are not public and are not searchable. The tweets we post are only viewable by the persons we have been approved to follow @CarrPrimary. Also, when a follower is verified their profile is accessed so that we can "Turn Off Retweets" on their account, this means they cannot retweet one of our tweets.

STAFF PROFESSIONAL DEVELOPMENT

All staff receive E-Safety training annually and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- The ICT Co-ordinator carries out e-Safety training annually at the beginning of the academic year for all staff - any further advice, guidance and training is formally delivered to staff at staff meetings or twilight sessions as required.
- New staff receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and acceptable use agreement which is signed as part of their induction.
- The ICT Co-ordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority and others.
- All staff have been made aware of this E-Safety policy and their responsibility to apply it.
  All training is recorded by the school as part of the Child Protection/Safeguarding training log.

GOVERNOR TRAINING

Governors are expected to take part in e-Safety training/awareness sessions. This could be in one or more of the following ways:

- The ICT Co-ordinator will deliver training, from September 2016, to governors as a whole in a pre-arranged training session;
- Attendance at Gateshead Council's half day e-Safety training session which provides advice regarding integrating e-Safety into the curriculum;
- Attendance at a training session provided by an external provider like the National Governors Association;
- Participation in staff training sessions or information sessions arranged for parents.

All training is recorded by the school as part of the Child Protection/Safeguarding training log.

PARENT AND CARER AWARENESS RAISING

Many parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. 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. The school will therefore seek to provide information and awareness to parents and carers through:

- Parents' attention will be drawn to the school e-Safety policy in newsletters and on the school website.
- A partnership approach to e-Safety at school and home will be encouraged with parents. This may include offering parent meetings with demonstrations and suggestions for safe home internet use
- Parents are asked to read and confirm acceptance of the ICT Acceptable Use Policy and discuss its implications with their child, annually.
- Parents will be directed to the materials available to them on the Think U Know website (www.thinkuknow.co.uk)
- Parents will be encouraged to access the CEOP website which is available via the school's website.

LIABILITY

There are certain liabilities on any school when you open up new services such as internet use, email facility or social networking. The easiest way to explain this is to use an example:

After posting a tweet on Twitter, one of your followers posts a tweet with a link to an inappropriate image. A pupils clicks the link and is horrified, his parents decide to sue the school. Who is liable - the teacher or the school? Ultimately it is the school. This example may be a bit extreme but isn't outside the realms of possibility (a hacked account?). The point is, the school facilitated a service and a child was subjected to emotional distress. It could also be seen as cyberbullying or malicious communications. It doesn't matter, the school holds liability.

In order to mitigate any risk of liability to the school:

- Never be derogatory to any person, post content or link to materials that will bring the school name into disrepute.
- Never engage knowingly with a pupil outside of school.
- Always retain a personal/professional boundary with children at all times.
- Ensure the rules regarding photographs (as stated earlier) are followed.
- Use an appropriate and professional tone in all tweets/comments.
- Don't publish confidential or commercially sensitive material.
- Don't breach copyright, data protection or other relevant legislation.
- Don't use social media to air internal grievances.

SCHOOLS E-SAFETY SELF AUDIT

The ICT Co-ordinator and/or the Governor who is responsible for e-Safety will carry out termly audits with staff to ensure that they understand e-Safety.

This audit is also to be used by governors as a self-audit tool. A copy is available at Appendix 1.

Appendix 1

SCHOOLS E-SAFETY AUDIT

This self-audit should be completed by the School Governor responsible for e-Safety. Staff that could contribute to the audit include: Designated Safeguarding Lead, Headteacher/Deputy Headteacher, e-Safety Coordinator, SENDCO, a member of the Senior Leadership Team, School Business Manager.

Has the school an E-Safety Policy that complies with Gateshead guidance?	Y/N
Date of latest update:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for E-Safety is:	
The Designated Safeguarding Lead is:	
The e-Safety Coordinator is:	
Were all stakeholders (pupils, staff, parents/carers and governors) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-Safety training been provided for all members of staff?	Y/N
Do all members of staff sign an Acceptable Use Agreement on appointment?	Y/N
Are all staff made aware of the schools expectation around safe and professional online behaviour?	
Is there a clear procedure for staff, pupils and parents/carers to follow when responding to or reporting an e-Safety incident or concern?	
Have e-Safety materials from CEOP, Childnet and ULEAIS etc been obtained?	
Is E-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	
Are E-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	
Do parents/carers or pupils sign an Acceptable Use Agreement?	
Are staff, pupils, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	
Is internet access and filtering provided by an approved educational internet service provider which complies with DfE requirements (eg KPSN)?	
Does the school log and record all e-Safety incidents, including any action taken?	
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	

E-SAFETY CONTACTS AND REFERENCES

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Schools e-Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce - Report Abuse: www.virtualglobaltaskforce.com

Date this policy was formally reviewed and agreed by the Governing Body of Carr Hill Community Primary School:	14th July 2016
Signed on behalf of the Governing Body by:	Jeanne Pratt (Chair)
Signature:	JmPratt
Date:	14th July 2016
Date of next review:	Summer Term 2017