E-Safety & Data Protection Policy

Date of issue: December 2017
Review date: December 2018

The purpose of this policy is to ensure a clear strategy to address potential issues relating to children and staff and their safe use of electronic communication technologies, including web-based and mobile learning. These are an essential resource to develop the skills for life long learning. At school we have a responsibility to educate all pupils on e-safety issues, teaching appropriate and acceptable behaviour to ensure their safe and legal use of ICT both inside and outside of the classroom, including learning how to assess and manage risk for themselves.
Users are made aware of the potential risks associated with the use of some Internet technologies. Everybody in the school is responsible for maintaining the security of all sensitive data.
This policy and our Acceptable Use Agreements are inclusive of Internet use, technologies provided by the school and technologies owned by staff and brought onto school premises.
The named e-safety coordinator for the school is Miss Katherine Cooper (Headteacher).

Aims

- To ensure that the use of the Internet and new techologies in school is well managed and carefully monitored
- To promote effectiveness of the Internet and new technologies in contributing to staff and children's learning
- To ensure that new technologies are equally available to all children at an appropriate level to support their learning
- To promote an understanding of the Internet and the need for responsible and appropriate use
- To ensure safe use of the Internet and new technologies by all staff and children

Internet use in School

Every class currently has access to the Internet on PCs, Tablet Pcs, laptops and ipads through wireless Internet connections. Internet use is an integral part of the curriculum and is a vital tool for learning. Our duty is to ensure that all children have opportunities to be involved in quality Internet access as part of their education. All access to the Internet in school is through the Hertfordshire Grid for learning and this offers filtered access through the local education authority's Intranet, blocking inappropriate websites. HGfL web based activity is monitored and recorded. Access to the Internet will be primarily through teacher demonstration, supported by directly supervised access to specific approved materials, with clearly defined learning objectives.
Using search engines is carefully managed by staff to ensure appropriate use and suitable information is accessed. Children accessing the Internet in school are given very clear instructions to use websites in "Favourites" and no others, unless specifically instructed by a member of staff.
Staff use the Internet to support their cross curricular teaching and its effectiveness and its contribution to learning is monitored and evaluated (as with all other resources). Any breach of this policy for appropriate use will be reported to the Headteacher.

Use of e-mail

The children in school do not have individual email addresses although whole class addresses may be used if a suitable opportunity arose. Children need to learn how to write email effectively and this is only in use with close adult supervision, conducted through HGfl 'Office 365 Mail'.
Staff have access to email and may use it with the class for specific purposes. This demonstrates this facility to the children. They can share in the composition of a message and experience receiving electronic replies.
All teaching staff have an email address through Hgfl (domain: cunninghaminfants. User name: first initial plus surname). To protect staff and ensure information is secure, these addresses are to be used for all school business passed by email. Personal email addresses must not be used.
Staff sending emails to external organisations should cc the school office - admin@cunninghaminfants.herts.sch.uk
All staff take responsibility for actively managing their email account by organising, archiving and deleting.
All access to school email is governed by this policy.
Emailing confidential information is only undertaken with consent from the Headteacher and will only be sent as an encrypted attachment.

E-safety in the curriculum

Esafety is taught as an integral part of the Herts ICT scheme of work (available on Dropbox).
All children using the Internet in school are taught correct and effective use of this resource. There is a risk for young children of inadvertent access to inappropriate material. Therefore, they are also taught that some of the information available on the Internet is not appropriate for children and that if they see any images or information of this nature they are expected to close the window and speak to the adult in class immediately. Children are regularly involved in discussion about safe use of the Internet at home and we recommend strongly that they should only use the Internet when an adult/older carer is present.

Responsibilites of school staff

All staff sign an acceptable use form to ensure the code of conduct is followed.
ICT use is carefully monitored, and Internet use in particular, and all staff take responsibility for this.
Any breach of this code of conduct is reported to the Headteacher.
Staff will ensure that the copying and use of Internet materials complies with copyright law.
School laptops in use off school premises will only be used in accordance with our Acceptable Use policy for ICT, agreed by all staff.
Information transported between school and other premises by use of pen drive/memory stick will be deleted immediately after transfer. Portable devices must be encrypted and/or password protected.

Protecting personal, sensitive, confidential and classified information.

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential and classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential or classified information contained in documents you fax, copy, scan or print
- You must not post on the internet personal, sensitive, confidential or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Selecy PINs to ensure that they are not easily guessed eg do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, included any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Staff training

All staff have been made aware of their responsibilities relating to the safeguarding of children within the context of e-safety. All staff receive systematic regular training through discussion, reference to LA advice and a record of agreed actions and reminders.

School website
The school has developed its own website, offering information about the school to children, parents and the wider community.
Children's work is published on the website, unnamed.
Photographs of groups of children are unnamed and children are not photographed and named individually. On their child's entry to school, all parents have the opportunity to request that photographs of their children are not used at all on the Internet.
The school website is managed by the admin assistant and is monitored by the Headteacher. School employs the services of an independent web consultant who also monitors to web traffic and troubleshoots.

Management of information systems
The senior management team are fully aware of the need for regular review of the security of information systems within the school.
All internet connections are arranged through the technical support team, part of Hertfordshire Education authority. Our ICT technician supports the school with ICT security both in the classrooms and the offices.
Virus protection is regularly monitored and updated.
All school data is protected by confidential passwords.
All users are expected to work reasonably and responsibly.
No personal details about pupils are included in any email communication unless required in encrypted form.
Information about Privacy Notice has been distributed to all parents and is available on the school website.

Data security
All school data kept on computers is password protected to ensure security.
All mobile equipment containing data is kept locked.
Laptops/portable devices are locked away or must remain with the person at all times.
All passwords are set by individual staff members at first log on and only shared with authorised ICT support staff when necessary.

Use of digital images
Images of children in school (photographs and video) are used as a valuable teaching, learning and recording tool. These images are only used within school and will not be transferred using any personal portable media without permission from the Headteacher. All photographs of children on the website or for other outside purposes are only used when written permission has been given by parents/carers. Images are not saved on a computer for longer than is necessary and staff take responsibility for deleting files on class based hardware. Images of the children are stored on the school's network. Pupils and staff are not permitted to use personal portable media for storage of images. Class teachers have the responsibility of deleting the images when they are no longer required. Mobile devices need to be turned off by all visiting parties including parents. Mobile devices may not be used during any production or school event involving children.

Social Media
Facebook, Twitter, Blogging and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook, Twitter and Blogging to communicate with parents.
- Teachers are able to Blog using their own log in and passwords
- Office staff are able to Blog using their own log in and passwords
- Facebook updates are linked to each blog
- Blogs are monitored by the Headteacher on a regular basis

Risk assessment
The school will take every precaution to ensure that children only have access to appropriate material. However it is not possible to guarantee this and the school does not accept liability for material accessed or any consequences arising from Internet use.

E-safety incidents

All e-safety incidents will be dealt with by a senior member of staff, in collaboration with the e-safety coordinator (Miss Katherine Cooper - Headteacher), and recorded in the incident log.
Any complaint about staff misuse will be referred to the head and recorded in the incident log.

Involvement of parents
Through parents information evenings, parents are made aware of the school's measures to ensure the safety of their child whilst using ICT in their learning and to raise awareness of the need to be vigilant at home. School makes available the latest advice from the LA on the school's website.
Internet issues arising will be dealt with carefully, involving the parents as appropriate.
Suitable websites are occasionally suggested to parents to support their child's work/homework and we recommend that this access is supervised.
Parents sign a home/school agreement when their children start in the school, giving consent for images of children to be used on the website. Staff are aware of the children whose parents have not given consent.

Involvement of Governing body
Governors are updated by the Head and/or e-safety coordinator to ensure clear understanding of issues and strategies for e-safety in our school. This policy protects the safety of the whole school community.

Equal opportunities
All pupils will be given consistent messages about safety to enable them to make appropriate decisions and choices.
Additional teaching and regular reminders will be provided for pupils to reinforce these messages as appropriate, particularly for children who may need further explanation to reinforce their knowledge and understanding of safety issues. Internet activity is carefully planned and well managed for all children.

Disposal of redundant ICT equipment
All redundant ICT equipment is disposed of using a service provided by SITTS or INTERM.

Appendix A

Cunningham Hill Infant School
Acceptable Use Agreement / eSafety Rules

For pupils

- I will only use the Internet and email with an adult.
- I will only click on icons and links when I know they are safe.
- I will only send friendly and polite messages.
- If I see something I don't like on a screen, I will always tell an adult.

For parents

- I will support the school approach to online safety
- I will ensure that my activity online or on social media is not offensive or disrespectful to other members of the school community
- I understand that any mobile device should not be used on school premises and that the school does not consent to recording of conversations with staff

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like further explanation, please contact Miss Cooper.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂----------

Parent/ carer signature

We have discussed this document with …….....(child's name) and we agree to follow the eSafety rules at Cunningham Hill Infant School

Parent/ Carer Signature ……

Class …… Date ……