# Heritage Park Primary School
# E-Safeguarding Policy

At Heritage Park Primary School, we understand that the virtual world is constantly changing and that we need to be aware of the risks. It is essential that all stakeholders in school use technology appropriately, safely and legally.

We have a responsibility to ensure we teach children the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet or other related technologies. E-Safety is a child safety issue not an ICT issue.

The school governing body have responsibility for ensuring that the school has an E-Safety policy for ICT and that this policy is reviewed annually. The Head will ensure that there is a designated staff member for E-Safety. The E-safety co-ordinator will ensure that staff discuss safety issues with the children and ensure the technology used by children operates using suitable anti-virus protection and the internet connection is filtered through the regional broadband consortium.

Pupil Acceptable Use Agreements are displayed near all the PC's and laptops that children use in school and an agreement is signed by parents, pupils and staff before access to the Internet is granted.

An E-Safety Incident Log will be maintained by the E-Safety co-ordinator and they will report to the Headteacher on issues as they arise.

## Searching for images safely online

While teachers may find search-engine image searches useful in lesson preparation, they should be used with care and caution in a `live' classroom setting. Children should not access search engines such as `Google Images' in school and should be aware of how to deal with inappropriate results if they access it from home.

## The importance of evaluating and reviewing online resources

Teachers should critically evaluate websites when selecting resources for use in the classroom, and pupils should also be taught these skills as part of their digital literacy skills development.

## Safe and effective searching online

Various search tools and techniques can help to locate relevant information quickly, easily and safely online. A good understanding of search tools and techniques will help children to easily find relevant content.

The school uses the filtering system provided by Peterborough City Council. This operates at a high security setting to try and ensure that inappropriate website content is blocked.

## How to minimise `cyberbullying'

Children will be educated about the potential risks issues from bullying by text message, email or online via websites and social networking sites. This will help to reduce the risks and provide an open culture where bullying of this nature can be freely reported and discussed, whether it takes place in school or elsewhere. The school has a policy of dealing with cases of cyberbullying in the same way that we would deal with any other cases of bullying.

## Mobile technology and e-safety

We do not permit children to bring mobile phones into school. Where it is necessary for them to bring one in, children will need to hand it into the school office on arrival. Under no

circumstances are staff permitted to take photos of children on their mobile phones. Staff mobile phones will be kept in the staffroom during the day.

Some potential issues with mobile technology are:

- Children are at risk from making inappropriate `friends', perhaps providing information or arranging a meeting that could risk his or her safety or the safety of others.
- It is difficult for parents to supervise access and contacts in the same way as they would a computer in the home.
- Mobile phones are typically always on and hence the owner is always contactable and, potentially, always vulnerable.
- Children may be exposed to material that is pornographic, hateful or violent in nature, or encourages activities that are dangerous or illegal.
- Mobile phones are also used as a tool by bullies, using text messages, and images of people being photographed without their consent or knowledge, as a tool to torment their victims.
- Photographs can inadvertently include clues as to an individuals location, such as the school name in the background which, if distributed inappropriately could lead to the risk of contact by strangers.
- Other concerns include social networking, with many young people posting content and images online of themselves and friends. The level of personal information young people are making available, particularly with regard to their daily routines can also cause issues.
- Additionally, the increasingly desirable nature of mobile phones means that young people owning them may become targets for theft.
- A child could do something that has legal or financial consequences such as giving out a parent's credit card details or doing something that contravenes another person's rights.
- Easy access to chargeable content and premium rate services in the form of games, downloads, ringtones, logos and other services all of which are particularly attractive to children and young people.
- Spam by text message is also a problem, meaning that children and young people could be tricked into revealing personal information.

**Securing and preserving evidence if illegal online activity is suspected**

Following any incident that may indicate that evidence of indecent images or offences concerning child protection may be contained on the school computers, the matter should be referred to the police at the earliest opportunity. Staff should not commence their own investigation prior to involving the police. This may result in the loss of valuable evidence both on and off the premises where suspects have become aware of raised suspicions. In some circumstances this interference with evidence may constitute a criminal offence. If a suspect computer is identified, it should not be used or viewed and the Head should contact the police. The police will be interested in obtaining `best evidence'. This, in reality, will be to forensically copy computers that may contain evidence of offences. This can be carried out discreetly out of hours, having minimal impact on the educational establishment.

If children or staff accidentally open unsuitable materials on a school PC the matter should be reported straight to the E-Safety co-ordinator. The co-ordinator will review the incident and decide on an appropriate course of action, applying sanctions as necessary. Staff will be debriefed as appropriate and relevant policies reviewed.

If a pupil or staff member discloses potential crimes involving computer-based media at home, again the police will normally try to obtain a forensic copy of their home computer to

preserve any evidence. This will be conducted discreetly and, in many cases, the computer will be returned quickly.

**Email in educational settings**

The school provide all staff and KS2 children with their own school email address. Individual accounts are created in KS2 as children gain the appropriate skills and knowledge to understand the security implications, and are able to manage their own online communications in a safe and responsible way.

The email addresses set up for the children follow a structure which runs the risk of unsolicited attention directed towards individual pupils from people outside the learning setting (by guessing a valid email address). Staff will discuss this with the children as a potential concern.

Staff email accounts are provided for all staff and may be used for school business or for limited personal use. If staff have Webmail accounts (such as Hotmail, etc.), they should not be used for school business. All school communications should always be sent and managed through a school email account, where appropriate filtering and monitoring can be employed, to minimise safety risks.

Pupils using webmail accounts outside of school should be taught to check for privacy statements when signing up for webmail accounts, not to consent to their details being shared with third parties to minimise the amount of spam they receive, and to make use of any inbuilt filtering tools.

Pupils should be taught appropriate writing and social conventions for using email, including suitable tone and language, so equipping them with the necessary skills to communicate effectively online.

Children should also be taught the appropriate behaviours to adopt if they receive an inappropriate or offensive email, such as closing it and seeking advice from a teacher or responsible adult, but never replying to it. This will allow the teacher or responsible adult to check the message, talk through the issues, reassure the pupil that it was not their fault that they received such a message, and take any other action as appropriate.

**Copyright issues for schools and colleges**

Under UK law, copyright material published on the internet will generally be protected in the same way as material in other media. Furthermore, each web page may contain several different copyrights if it contains text, music, graphics and so on. Many websites will include a copyright statement setting out exactly the way in which materials on the site may be used. When using websites in educational settings, children should be encouraged to look for copyright information and should be taught that many online resources may have been published illegally without the permission of the copyright owners. This may be particularly the case with media-based content such as music and videos. Any subsequent use of the materials may also be illegal.

Children should be aware that plagiarism (the theft of ideas and works from another author and passing them off as one's own) is not only cheating but, where sufficient is copied, illegal infringement of copyright also constitutes a criminal offence.

**Computer misuse in educational settings**

Incidents that constitute computer misuse include: unauthorised access to computer materials; unauthorised acts to impair operation of computer; making, supplying or obtaining articles for use in computer misuse offences; hacking or denial of service attacks.

Responsible online behaviour

The school will promote responsible online behaviour for learners and staff. Children and staff will be made aware that the following issues are not acceptable in school:

- Finding or guessing someone's password, then using it to gain access to data or services, or posing as other
- Deliberately changing or deleting files belonging to others
- Changing computer settings
- Deliberately introducing viruses onto the network

The school will monitor, report and respond to deliberate misuse of computer systems. Users will be made aware that system monitoring will take place randomly, and will be made familiar with possible sanctions for misuse. Depending on the seriousness of incidents, sanctions might include verbal warnings, temporary bans, involvement of parents and carers or, in extreme cases, permanent exclusion from the ICT facilities in school.

## Creating and maintaining safe websites

The school's website is created by an outside company called E4Education. All staff have access to the admin section of the website which allows them to add photos and work. The ICT subject leader reviews any changes made by staff before they are published.

Children will not be named individually on the website and will only be put onto the website if they have signed the relevant consent forms. Parents are asked to complete a form, when the children begin at the school, to give permission for children's images to be used.

## Embedding e-safety in the primary curriculum

E-Safety is embedded within the curriculum as well as being taught discretely. Staff understand the need to work together to ensure that a comprehensive, consistent and continuing programme of E-Safety education takes place across subjects, year groups and throughout the school.

Children will be taught what to do in the event of accidentally coming across inappropriate material in school, i.e., minimise the screen and go and tell an adult. They will need to ensure they are aware of the Responsible Internet Use rules displayed by the equipment in school.

## Data protection and education

The Data Protection Act 1998 will be adhered to in terms of data kept on the school systems. Staff will ensure data is collected with a specific purpose in mind. It will be kept secure and will only be kept for as long as it is relevant.

## Conclusion

By following this policy, we at Heritage Park Primary School seek to ensure that the children are aware of potential dangers and know how to use technology safely.

March 2012