E-SAFETY

A SAFEGUARDING POLICY

Policy Name	E-Safety
Contact Person	Head Teacher/ ICT Coordinator
Committee	Full Governing Body
Date of Approval	13.5.15
Date Last Amended	
Review Date	May 2016

Contents

Appendices (forms)

1. Introduction

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which, as in life generally, may be unsuitable. This policy will outline how the staff, pupils and Governors at Hollyfield Primary School will adopt strategies for the safe and responsible use of the internet.

The Internet is an open communications channel, available to all. Applications such as the Web, email and chat rooms along with the increase in mobile technologies that we now see in everyday life such as mobile phones, Ipad's, PSP's, Tablets, UMPC's, all transmit information over the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. Sadly e-mail and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

2. Safeguarding

In safeguarding our pupils we need to educate them about the benefits, risks and responsibilities of using information technology. We can quite easily block certain technologies or prevent access to particular websites. Is this educating our pupils? In the home, it is unlikely that parents would have safety and security features such as a firewall or strict filtering systems to prevent children accessing inappropriate content. With the sound advice we provide our pupils in school, we will not simply prevent access but teach them about the roles and responsibility that they have in using them and how to use them safely. By following the schools Acceptable Use Policy (AUP) individuals throughout our school will understand the responsibility that they play in keeping everyone safe while using Information Technology.

The E-Safety Policy will be used in conjunction with other mandatory school policies: child protection, health and safety, home–school agreements, behaviour (including the anti-bullying) and Data Protection Policy,

In order for us to work with our pupils and for the E-safety policy to work effectively we will need to look at a no blame culture where we accept that at times even the most innocent of web searches could return some inappropriate material. Pupils need to be confident in that reporting such incidents to an adult; they will be supported and not blamed.

Resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and

evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

To ensure the safeguarding of all stakeholders it is our school policy that personal mobile phones are not used during the school day when children are present. Staff are to use their class cameras or school iPads to take photographs and the internal school telephone system to make and receive necessary work related phone calls. If staff wish to check their mobile phones during the working day they must do so during designated break times and away from children; where possible mobile phones should be used in staff only areas.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet
- Describe how these fit into the wider context of our discipline and PSE policies
- Demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views and violence.

The school believes that the benefits to pupils from access to the resources of the Internet, far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

We feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents and carers.

Parents and carers will be sent an explanatory letter and the rules which form our Internet Access Agreement (See Appendix B)

3 . Using the Internet for Education

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 globe
- staff professional development through access to new curriculum materials, experts' knowledge and practice
- exchange of curriculum and administration data with Local Authority/Department for Education and Skills
- social and leisure use
- greatly increased skills in other subject areas such as Literacy

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons.

All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught.

Initially the pupils may be restricted to sites which have been reviewed and selected for content. They may be given tasks to perform using a specific group of web sites.

Pupils will have the opportunity to exchange information via email. They will be taught how to use the address book, how to attach files to an email and how to do so responsibly.

At times, information, such as text, photos etc may be "downloaded" from the Internet for use in pupils' presentations. E-safety lessons will be set to encourage pupils to view web sites and information with a critical eye.

In the event that a member of staff needs to use a personal device for educational purposes, such as music and language teachers who have their files on iTunes, they have permission to use their device to play these files only. The device can be used with a docking station but must not be connected to the school computers. The device can not be used for taking photos or any kind of recordings of the children.

4. Pupils' Access to the Internet

Hollyfield Primary School uses a filtered Internet Service, which minimises the chance of pupils encountering undesirable material. This filtering service is managed by the Birmingham Grid for Learning (BGFL) and Link2ICT.

- Hollyfield Primary School will only allow children to use the Internet when there is a responsible adult present to supervise. Pupils will be directed to websites by staff that will have checked out the suitability beforehand. If a URL is encountered that is deemed to be inappropriate, children are instructed to click on the 'Hector Button' and report to the teacher. The member of staff should report this to the ICT Leader who will investigate and refer to the appropriate authorities for the URL to be added to the list of blocked sites.
  Members of staff are aware of the potential for misuse, and will be responsible for reminding pupils of responsible Internet use regularly in lessons using the Internet (see Appendix A).

- Some emails deemed to be SPAM, Malicious, containing profanity or certain file types are filtered to the BGFL filtering account. Users will be able to request emails are release if they believe they are being withheld in error. These email types shall be automatically deleted after 14 days.

"Schools have a responsibility to educate young people and provide a safe learning environment. Increasingly, ICT is used as an integral part of teaching and learning, and evidence shows that it can have many important benefits. Schools, therefore, must also play a special role in educating children and young people about the safe use of the Internet and related technologies". **BECTA**
BECTA has been replaced by NAACE

To maintain personal safety pupils and staff at Hollyfield Primary School will work to the SMART rules.
S – Safe
M – Meeting
A – Accepting
R – Reliable

T – Tell

They will not:

- Post personal contact information about themselves or other people. Personal information includes names, address and telephone numbers etc.
- Attempt to gain unauthorised access to any computer, user account, files or folders which is beyond their security levels.
- Download programs or files without seeking permission from the ICT Leader or supervising member of staff
- Be allowed access to public or unregulated chat rooms.
- Use Personal USB or external hard disks to transfer data to and from the school network (School provides encrypted USBs to all teaching staff)

5. Expectations of Pupils using the Internet

- All pupils are expected to read and agree the Internet Use Agreement.
  We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.

Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.

- Pupils are expected not to use any inappropriate language in their email communications and contact only people they know or those the teacher has approved. They have been taught the rules of etiquette in email and are expected to follow them.

- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.

- Pupils should not access other people's files unless permission has been given.

- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

- No program files may be downloaded to the computer from the Internet. This to prevent corruption of data and avoid viruses.

- No programs on memory stick, disc or CD Rom should be brought in from home for use in school. This is for both data protection and security reasons.

- No personal information such as phone numbers and addresses should be given out and no personal arrangements to meet anyone will be made on the internet.

- Pupils choosing not to comply with these expectations will be warned, and subsequently, if further instances occur, will be denied access to Internet resources. They will also come under the general discipline procedures of the school which comprises an escalating set of measures including a letter to parents and withdrawal of privileges.

6. School Web Site Guidelines

A web site can celebrate good work, promote the school, and publish resources for projects and homework, and link to other good sites of interest.

- Information published will be accurate as at date of publish, and any inaccuracies that may occur will be corrected as soon as is possible.
- Parental photo consent will be sought for every child when they start at Hollyfield Primary School and only the children who have been given this consent will have their photographs shared on any public platform such as Twitter or the school website
- Where photos of pupils are to be uploaded their names will not be published.
- We will adopt a "photo, no name – name, no photo" approach and where possible only forenames should be used to minimise identification.
- Files uploaded will not refer to names. E.g. A photo of Joe Bloggs will not be joebloggs.jpg.
- Group photos will not contain a names list.
- Home information and e-mail identities will not be included on the website, only the point of contact to the school i.e. phone number, school address and all emails will be submittable through on site forms, no email address will be posted on the website.

7. Information System Security

- Virus detections will be dealt with promptly and where staff laptops are affected staff will be notified immediately and asked to bring the laptop into school ASAP for quarantine.
- All workstations and laptops in school will be updated with Microsoft critical updates each academic year or in the case of an urgent update this will be completed at the earliest opportunity.
- School security settings for the network, user accounts and folder structures will be reviewed regularly by the technicians.
- Any suspected access or security issue will be reported to the head teacher or the ICT Leader at the earliest possible time.

8. Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

9. Staff Laptops

- Teaching staff are allocated a laptop for PPA purposes.
- The laptop can be connected to the internet out of school and can be used for both personal and professional reasons, all of which must conform to the guidance within the e-safety policy and signed Code of Conduct and Laptop Use Agreement.
- Staff laptops will be returned to the school ICT technician annually or when requested to do so for critical updates and software installations.

10. Personal Data and Data Protection

- Pupil, Staff and any other personal Data will be stored securely and will be restricted to staff members who need the information.
- School data will be stored on the staff shared area to which only staff will have access.
- All staff will have a user account and understand the importance of a secure and strong password.
- Only Admin staff and SLT will have access to SIMS and accounts information.
- Staff will only have access to SIMS if their role requires it.
- SIMS access will be restricted for all users allowing them to view the data to which they are entitled.
- Access to the Admin network will be restricted for all users other than Admin staff.
- Personal Data will not be stored on shared drives to which children have access.
- Children's or Staff personal data will not be transferred offsite by means of memory pens unless specific permission is granted. If this data is necessary then the memory pen should be encrypted to prevent unlawful access.
- Data that can identify an individual should not be stored on staff laptops or offsite, and staff should be aware of the responsibility they have in minimising the risk for this data to be obtained by third parties.

11. Handling E-safety Complaints

Complaints of internet misuse will be dealt with by a senior member of staff.
Any complaint of staff misuse will be reported to and dealt with by the head teacher and SLT misuse by a designated Governor.
Complaints of a child protection nature must be dealt with in accordance to the school's child protection procedures.
Pupils and parents will be informed of the complaints procedure.

12. Plagiarism and Copyright Infringement

Staff need to be aware of copyright laws with regards to information on the World Wide Web. Government websites are generally free from copyright. However, all other websites are copy written. It is always good manners to send an email to the owner of the materials to confirm that they are willing to allow copying of pages of information. Projection or screen viewing of resources is permitted.

Staff are encouraged to look around for free information and use visual projection when accessing resources from the Internet.

13. British Values

At Hollyfield Primary School, Staff and Governors are committed to the safety and welfare of all pupils and will ensure that, through the robust implementation of all safeguarding policies, that all pupils are protected from any potential exposure to extremism and radicalisation.

We will ensure that all our pupils, especially those with SEND, will be fully supported academically and socially to ensure that no pupil is at risk of bullying or any other form of discrimination.

14. SIMs

SIMs allows class teachers to take online registration enabling instant and up to date records for office staff on the attendance of pupils. SIMs also allows access to personal data of pupils such as attendance information, emergency contact details and address information. It is therefore vitally important that when staff use this system they logout once registration is complete. Staff must never allow children access to the system unattended and must never divulge the username/password to pupils.

15. Useful Web Links

www.childnet.com
www.thinkuknow.com
www.thegrid.org.uk/eservices/safety
www.naace.co.uk
www.ceop.police.uk

Appendix A- Internet Use Agreement – Pupil Version

All pupils and their parents / guardians will be asked to read and sign an agreement covering the expectations we have of pupils using the Internet in school.

Responsible Internet Use

We use the school computers and internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- I will ask my teacher before entering any website that I want to look at.
- I will not let anyone know my password or login name.
- I will not look at or delete other people's work.
- I will not bring my own memory sticks or CD Roms into school without asking my teacher first.
- I will only e-mail people that the teacher allows me to.
- The messages I send will be polite and sensible.
- When sending e-mail, I will not give my home address or phone number, or arrange to meet anyone.
- I will tell my teacher if I get an email from someone I don't know.
- If I see anything I do not like on the computer, I will tell a teacher immediately.
- I know that the school will check my computer files and can check the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

Pupil Name……Date……Signed…….

Appendix B

Dear Parents/Carers

Responsible Internet Use

As part of your child's curriculum and the development of ICT and Computing skills, we regularly provide supervised access to the Internet. We believe that use of the World Wide Web and email is worthwhile and is an essential skill for children as they grow up in the modern world.

The school has revised the E-safety Policy to ensure it is up to date with current technologies and Internet use and is intended to ensure we make the most of the opportunities that the Internet offers whilst minimising the possible risks.

This Policy requires all pupils to understand and sign an Internet Acceptable Use Agreement. We think it is important that you, as parents and carers should also be aware of the ways we expect children to behave when using the Internet in school and the steps that are taken to keep children safe online.

Please would you read the attached Internet Acceptable Use Agreement with your child and sign and return the consent form so that your child may use the Internet at school.

Should you wish to discuss any aspect of the Internet, please do not hesitate to contact me.

Yours sincerely

Appendix C
ICT-Esafety Staff User Agreement

To ensure that staff are fully aware of their responsibilities with respect to ICT use, they are asked to sign this acceptable use agreement.

- I understand that the network is the property of the school and agree that my use must be compatible with my professional role.

- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Head teacher.

- I understand that the following will be deemed as inappropriate and members of staff or individuals using the ICT infrastructure at Hollyfield Primary School who are found to have breached this policy or attempted to do so will be dealt with under the Hollyfield Primary School discipline procedure and this could lead to criminal prosecution as well as dismissal. Accessing, browsing or searching for, storing, downloading or forwarding any materials, be they word, image, audio or data which could be deemed:

  - obscene
  - offensive
  - sexual
  - politically offensive
  - be an act which may bring Hollyfield Primary School, Birmingham City Council or the individual into disrepute.
  - make a contribution to a newsgroup chat room or other similar medium.
  - be considered as running a private business eg selling or advertising.
  - an infringement of copyright (including images, text, music or video in any format)
  - use of web based emails other than that provided by the school.
  - make any attempt to circumnavigate the security and protection in place on the networks or computers.

- I understand that it is our school policy that mobile phones are not used during the school day when children are present:
  - I will use the class camera or iPads to take photographs
  - I will use the internal school telephone system to make and receive work related phone calls.
  - If I wish to check my mobile phone during the working day I will do so during designated break times and away from children
  - Where possible I will use my mobile phone in staff only areas

I understand and agree that school will monitor the network and Internet use to ensure policy compliance.

- I will respect ICT systems security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will not install any software or hardware without permission.
- All memory sticks, flash discs and other transportable media should be encrypted. I will only e-mail, to my own email account if the transmission does not contain any data about an individual, if this is the case, then this data should only be dealt with on school owned equipment.
- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system.
- I will take all reasonable precautions to secure data or equipment taken off the school premises and report any compromises immediately to the Head Teacher.
- I will report any incidents of concern to the school Designated Child Protection Officer as appropriate.
- I will ensure that my electronic communications with pupils are compatible with my professional role and cannot be misinterpreted.
- I will promote e-safety with the pupils that I work with and will help them to develop a responsible attitude to ICT use.
- Disposal of software/hardware used by the school shall only be carried out through the IT disposal policy will need to be signed off by the IT technician and the Bursar. Any equipment disposed of in any other way may be deemed as theft.
- I will respect copyright and intellectual property rights.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed ……Capitals…….

Date …….