**Park Hill Primary School**

***'We aim to bring out the best in everyone.'***

**Internet and E-Safety Policy**

**2nd OCTOBER 2017**

**Review date : 12 months from issue**

## 1. RATIONALE

Birmingham LEA and Park Hill School believe in the invaluable educational benefits of curriculum Internet use, both in school and at home. The school management recognise the risks and dangers associated with use of the Internet and plan accordingly to ensure appropriate, effective and safe pupil use. This policy outlines our purpose in providing e-mail facilities and access to the Internet at Park Hill and explains how the school is seeking to avoid the potential problems that unrestricted Internet access could give rise to. BECTA also suggests that school policies include pupils' own hand-held devices which may be brought into school.

The following document is based on E-Safety policies produced by Birmingham, Kent and Co. Antrim LEAs and guidance from BECTA.

## 2. SCHOOL CONTEXT

Park Hill is a 3 form entry school with 650 children aged between 3 and 11 years old. Our pupils are from multi-cultural, multi-faith, socially diverse backgrounds. Park Hill is an inclusive school, offering an education to all our children that enables them to enjoy learning and achieve to their full potential.

## 3. CORE PRINCIPLES OF INTERNET SAFETY

The Internet is now the world's largest source of information and a primary means of communication. Unmediated Internet access brings with it the possibility of placing pupils in embarrassing, inappropriate or even dangerous situations. This policy is aimed at ensuring responsible use and the safety of pupils.

This policy is built on the following 5 core principles:

### A) GUIDED EDUCATIONAL USE

- Curriculum Internet use should be planned, task orientated and educational within a regulated and managed environment.
- Directed and successful Internet use will reduce opportunities for activities of dubious worth.

### B) RISK ASSESSMENT

- While pupils must be protected from violence, racism and exploitation, they must also learn to recognise and avoid these risks.
- The school must be fully aware of the risks, perform risk assessments and implement a policy for Internet use.
- Pupils need to know how to cope if they come across inappropriate material.

### C) RESPONSIBLITY

- Internet safety depends on staff, governors, advisers, parents and pupils themselves taking responsibility for the use of the Internet and other communication technologies such as mobile phones.
- There should be a balance between educating pupils to take a responsible approach and the use of regulation and technical solutions.

### D) REGULATION

- Regulation is required for certain cases, such as access to unmoderated chat rooms, to which access is denied.
- Fair rules, clarified through discussion and prominently displayed at the point of access will help pupils to make responsible decisions.

### E) APPROPRIATE STRATEGIES

- The strategies described below aim to help ensure responsible and safe use.
- Strategies are based on limiting access, developing responsibility and on guiding pupils towards educational activities.

## 4. E-SAFETY POLICY

### A) HOW WE USE THE INTERNET

- To raise educational standards; promote pupil achievement; support professional work of staff; enhance school's management information and business administration systems.
- As part of a statutory curriculum and as a necessary tool for staff and pupils.
- All children are entitled to use the Internet and must use it in a responsible and mature manner.

### B) WHY WE USE THE INTERNET

- To provide access to educational resources.
- To support links with other schools and pupils worldwide.
- To support staff professional development opportunities.
- To communicate with colleagues (internally and externally), professional associations and support services.
- To share work and contributions with the world wide educational community.
- To access technical support.
- To exchange curriculum and administration data with the LEA and DfE.

### C) USING THE INTERNET TO ENHANCE LEARNING

- The school's Internet access includes filtering appropriate to our pupils' age.
- Pupils are taught about acceptable Internet use and are given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning.
- Internet access is supervised at all times.
- Teachers must research and review web sites.
- A selection of appropriate sites should be saved in a folder on the common drive.

### D) EVALUATING INTERNET CONTENT (INCLUDING YOUTUBE)

- Upon discovering unsuitable sites, the URL (address) must be reported to the ICT co-ordinator.
- Staff must comply with copyright law when generating resources.
- Pupils should be taught to evaluate the quality and reliability of information from the Internet.
- Internet searches should be constructive and guided, using primaryschoolict.com.
- Staff *must* preview YouTube videos prior to showing them to pupils.
- Staff *must* open YouTube links through www.safeshare.tv, which removes advertising content or through ActivPrimary or LearnAnywhere

### E) EMAIL

- Pupils do not currently have access to an individual email address.
- Pupil have access to an internal messaging system with the VLE.
- Messages are monitored by the ICT leader.
- Messages flagged as inappropriate are sent to the ICT leader. Incidents may be referred to the Head Teacher.
- Staff may only use approved email accounts on the school system.
- Staff should immediately report any junk or offensive emails to the ICT technician.
- Emails sent by staff to an external organisation are professional documents. They should be carefully written and viewed in the same way as a letter written on school headed paper.
- Staff must not forward chain letters/emails.
- Staff should not open attachments or click links within emails from an unknown source.
- Staff should not open emails with a blank "subject" field if from an unknown sender.

### F) SCHOOL WEBSITE

- The point of contact on the school website should be the school address, email address and telephone number.
- Staff or pupils' home information will not be published.
- Photographs of staff and pupils are carefully selected and written permission from parents or carers is sought before publishing photographs on the school website.

- Pupils' full names will not be used anywhere on the web site, particularly in association with photographs.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

**G) HANDHELD DEVICES, CHAT ROOMS AND INSTANT MESSAGING**

- Pupils are not permitted to bring in handheld devices (including mobile phones) into school unless a written request is made by parents and approved by the head teacher. In these cases, inexpensive mobile phones must be provided (no smart phones). These must be handed in to the school office at the start of the day, where they will be kept securely before collection at 3.15pm.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden, and may even constitute a criminal offense.
- Staff **must not** use personal equipment to photograph or record children.
- Pupils will not be allowed access to chat rooms or instant messaging.
- Pupils may use handheld tablets under supervision by teaching staff.
- Staff **must not** keep mobile phones with a camera facility on their person during working hours.

**H) USING BLOGS**

- Creating a blog can provide an excellent platform for pupils to share work with other pupils around the world.
- Blogs should be created in a secure way, so that the teacher or supervising adult can approve all posting prior to them being visible by pupils.

**I) RISK ASSESSMENT**

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils**.** The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked up nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school, nor BCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- The head teacher will ensure that the E-Safety policy is implemented and compliance with the policy monitored.
- The school will work in partnership with parents, the LEA, DfE and the ISP to ensure systems to protect pupils are reviewed and improved.

**J) TEACHING OF E-SAFETY**

- Rules for Internet access will be displayed in all rooms where computers are used.
- Pupils are informed that Internet use will be monitored.
- Pupils will be taught E-Safety discretely prior to accessing the internet at the beginning of the school year and throughout the year during class assembly time.
- The school will use a variety of resources and programmes to deliver E-Safety.
- Children are taught the potential risks of using a games console to access the Internet.
- Children are taught about the purposes and nature of social media sites such as Facebook and Twitter. It is made explicit that these services are not designed for children and the risks and danger of such sites is explained.
- Pupils are signposted to the www.beatbullying.org website and ChildLine through posters if they feel like they need to discuss an issue externally.

**K) STAFF**

- All staff are governed by the content of this policy and by the terms of the "Responsible Computer Use" appendix.
- Staff are required to agree with an Acceptable Use Policy when accessing school computers.
- All staff will be provided with a copy of the policy, and its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff training in safe and responsible Internet use and on the school E-Safety policy will be provided as required.
- Agency supply teachers are provided with a generic name and password.

**L) ICT NETWORK SECURITY**

- The school ICT systems will be reviewed regularly with regard to security. This is managed by the IT support provide (EdIT Ltd)
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LEA, particularly where a wide area network connection is being planned.
- Files held on the school's network may be checked periodically.
- The IT co-ordinator / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

**M) ENLISTING PARENT SUPPORT**

- Parents' attention will be drawn to the school E-Safety Policy in newsletters and the school website.
- Internet issues will be handled sensitively so as to inform parents without undue alarm.

**N) COMMUNITY USE OF THE INTERNET**

- Adult users will need to agree with the acceptable use policy before using school facilities to access the Internet.
- All community users will be given a generic username and password.
- Parents and carers of children attending after school clubs will be made aware of the school policy and be expected to adhere to it.

## 4. PROCEDURE FOR INCIDENT RESPONSE AND REPORTING

Even with the policies and technological measures in place, the school should be prepared to respond to instances of misuse or other breaches of policy.

- Responsibility for handling incidents is held by the Head Teacher.
- Pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
- All incidents will be recorded in the school's E-Safety incident book, to be held by the delegated person.
- If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handing incidents involving children will be taken by the ICT Co-ordinator and the Child Protection Officer in consultation with the Head Teacher and the pupil's class teacher. All the teaching staff will be made aware of the incident in Pupil Awareness at a Staff Meeting if appropriate.
- If one or more pupils discover (view) inappropriate material the first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue.
- If staff or pupils discover unsuitable sites the ICT co-ordinator will be informed. The ICT co-ordinator will report the URL (address) and content to the Internet Service Provider and the Local Authority. If it is thought that the material is illegal, after consultation with the Local Authority, the site will be referred to the Internet Watch Foundation and the police.
- Sanctions will be in line with the school's behaviour policy and will include removal of internet access for a period.
- Any staff misuse will be referred to the Head Teacher.

**APPENDIX 1**

# IT Acceptable Use Policy (Pupils)

## Park Hill Primary School

These rules help us to be fair to others and to keep everyone safe

- I will only use my own login and password for the school network.
- I will only use the Internet under instruction from my teacher.
- I will only look at my own (and shared) files. I will only delete my own files.
- I understand that I must not bring memory sticks into school without permission.
- I will not use chat or instant messaging services.
- If I see anything I am not happy with or receive messages I don't like, I will tell my teacher immediately.
- I understand that the school may check my device's files and the Internet sites I visit.
- I must treat all equipment with care and respect.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

**APPENDIX 2**

# IT Acceptable Use Policy (Staff and Volunteers)

## Park Hill Primary School

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

### For my professional and personal safety:

- I understand that the school can monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person (DSL)
- I will not keep my personal mobile phone or personal photographic equipment on my person during working hours.

### I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

## The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless consultation has been taken with IT technician
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

## I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy ICT equipment in school, but also applies to my use of school / academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include: a warning, a suspension, referral to the Local Authority and in the event of illegal activities the involvement of the police.

# APPENDIX 3

## References

**More general information about e-safety can be obtained from the following organisations: -**

### Particularly for Parents and Children

**Bullying Online** — **www.bullying.co.uk**
Advice for children, parents and schools

**FKBKO - For Kids By Kids Online** — **www.fkbko.co.uk**
Excellent Internet savvy for kids; KS1 to KS3

**Kidsmart** — **www.kidsmart.org.uk**
An Internet safety site from Childnet with low-cost leaflets for parents.

**Think U Know?** — **www.thinkuknow.co.uk**
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

**Family Guide Book (DfE recommended)** — **www.familyguidebook.com**
Information for parents, teachers and pupils

### Particularly for Schools

**NAACE / BCS** — **www.naace.org (publications section)**
A guide for schools prepared by the BCS Schools Committeeand the National Association of Advisers for Computer Education (NAACE)

**Internet Watch Foundation** — **www.iwf.org.uk**
Invites users to report illegal Web sites

**Data Protection** — **http://www.ico.gov.uk/**
New Web site from the Information Commissioner

**Kent Web Skills Project** — **www.kented.org.uk/ngfl/webskills/**
Discussion of the research process and how the Web is best used in projects.

**Copyright** — **www.templetons.com/brad/copymyths.html**
Irreverent but useful coverage of the main aspects of copyright of digital materials, US-based.

**DotSafe – European Internet Safety Project** — **http://dotsafe.eun.org/**
A comprehensive site with a wide range of ideas and resources, some based on Kent work.

# APPENDIX 4

## Further Guidance and Legal Context

The following legislation is relevant to schools:

**Data Protection Act 1984/98**
Concerns date on individual people held on computer files and its use and protection.
*http://www.opsi.gov.uk/acts/acts1998/19980029.htm*

**Computer Misuse Act 1990**
Including hacking and denial of service attacks.
*http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm*

**Copyright, Design and Patents Act 1988**
Makes it an offence to use unlicensed software.
*http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm*

**The Telecommunications Act 1984**
Including illegal material on, or transmitted via, the web and electronic communications.
*Not available online*

**Protection of Children Act 1978, as amended by Section84 of the Criminal Justice and Public Order Act 1994**
Including indecent images of children.
*http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm*

**The Obscene Publications Act 1959 and 1964**
Including illegal material on, or transmitted via, the web and electronic communications.
*Not available online*

**Sexual Offences Act 2003**
Including grooming
*http://www.opsi.gov.uk/acts/acts2003/20030042.htm*

**Malicious Communications Act 1988**
Including harassment, bullying, and cyberstalking.
*http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm*