Park Street C of E Primary School & Nursery

Together we Learn

Together with God

[redacted]	
Version	1.0
Name/Department of originator/author:	E-Safety Policy
Name/Title of responsible committee/individual:	Mr R McDonough
Date issued:	January 2017
Review frequency:	Annually
Target audience:	All members of the school community

The governing body shall conduct the school with a view to promoting high standards of educational achievement.

Park Street Primary School is committed to eliminating discrimination, advancing equality of opportunity and fostering good relations between different groups. These factors were considered in the formation and review of this policy and will be adhered to in its implementation and application across the whole school community.

Park Street Primary School will promote the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs and will actively challenge any member of the school community expressing opinions contrary to fundamental British Values, including ‘extremist’ views.

Version	Date	Notes
V1.0	Jan 2017	Reviewed by Mr McDonough.
V1.1	April 2019	Reviewed by Mr McDonough

Together we Learn

Together with God

PARK STREET C OF E PRIMARY SCHOOL AND NURSERY

E-SAFETY POLICY – April 2019

This policy is intended to raise awareness of the safety issues associated with electronic communications as a whole and to ensure best practice by every member of the school community. It has been produced with reference to guidance from Herts Grid for Learning [HGfL].

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-safety policy operates in conjunction with other policies including those for ICT acceptable uses, Behaviour, Anti-Bullying, ICT and other curriculum policies and Data Protection.

The Assistant Head, Rawdon McDonough is the E-Safety Co-ordinator.

The E-Safety Policy and its implementation will be reviewed annually.

The E-safety acceptable uses policy will be reviewed annually.

Why Internet use is important

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions
- Internet use is part of the statutory curriculum and a necessary tool for learning
- Internet access is an entitlement for children
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security

How does Internet use benefit education?

- Benefits of using the Internet in education include:
- access to world-wide educational resources including museums and art galleries
- inclusion in the wider network of all UK schools
- educational and cultural exchanges between pupils world-wide
- vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for pupils and staff

- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet is designed expressly for pupil use and includes filtering appropriate to the age of pupils
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and ability
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

How will pupils learn how to evaluate Internet content?

- Our school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of on-line materials is a part of every subject

Managing Information Systems

- The security of the school information systems will be reviewed regularly
- Virus protection will be updated regularly. Completed by IntermIT
- Security strategies will be discussed with the HGfL and our technical support provider, IntermIT
- Personal data sent over the Internet will be secured
- Portable media may not used without specific permission followed by a virus check
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail
- Files held on the school's network will be regularly checked
- The ICT Subject Leader and IntermIT technician will review system capacity regularly
- School reports should be accessed from the school. They should not be stored on memory sticks
- All staff with access to SIMS data will follow the security protocols set

Roles and Responsibilities

The school's access to the Internet is through the Hertfordshire Grid for Learning, which filters the World Wide Web. Responsibilities are as follows:

- **RM** – as the contractors who provide the HGfL service RM are responsible for implementing the policy as directed by Herts County Council
- **Herts County Council** – in consultation with advisory and teaching colleagues, and with the Hfl Steering Group, the Hfl co-ordinator is responsible for agreeing a safety policy for the service and communicating this effectively to the internet provider.
- **Schools** – are responsible for ensuring that pupils and their parents are aware that the Hfl is a safe on-line environment for learning. They are also responsible for ensuring that pupils are aware of what to do should they ever feel uncomfortable with any web material accessed or e-mail message received. This policy sets out our approach to these issues.
- **Pupils** – should only use the Hfl services to promote their own education in accordance with this policy.
- **IntermIT**---are responsible for the upkeep of the server and updating the system when required.

Filtered access to the World Wide Web

The filtering of the World Wide Web by RM is a two-stage process. Information requested from the Internet has to pass through both stages before it will be sent through to school.

Stage 1 - Deny Lists
Whenever someone in a Hertfordshire school types in a World Wide Web address, or clicks on a link to an address, the request for that information is first passed to a computer, called a proxy server, at the centre of the HfL core network. This computer checks to see if the requested address is listed as being unsuitable. If it is on the list, instead of seeing the requested page the user will see a message indicating that the material on that page is thought to be inappropriate for use in schools. These deny lists are updated automatically every few days.

Stage 2 - The Dictionary
If it is not listed the page will be retrieved from wherever it may be on the Internet but as it comes back through the central computer the words contained on that page are checked. Certain words have a score associated with them and if the total score for any page reaches a given total then that page will not be sent through to the requesting school. Once again a message indicating the unsuitability of the material on that page is sent to the user instead.

However, the RM filtering cannot be 100% perfect because different people will draw the line about what is suitable and unsuitable for schools in different places and because the Internet changes so quickly that it is difficult to keep the deny lists up-to-date.

The RM proxy server records all the websites visited.

Our pupils are instructed that if they come across an internet page which they find distasteful, uncomfortable or threatening, they are to close the page and report it to their teacher immediately. He/she will speak to the E-safety co-ordinator (Mr McDonough / Assistant Head) He will arrange for the RM Helpdesk to be contacted – they will be able to instantly add the page to the deny lists.

Any material that the school believes is illegal is referred to RM

The school will work in partnership with RM, to ensure systems to protect pupils are reviewed and improved.

How is e-mail managed?

The security of the school’s email service is ensured by Intermit by:

- **The structure of the addresses themselves**

- **The screening of inappropriate words** - If an e-mail user sends a message with some mildly rude words then the message will be delivered but the recipient will also get a note warning him/her that there is some mildly inappropriate content

  If a message containing not-so-mild rude words is sent by a grid e-mail account or to a grid e-mail account then it will not be delivered. The sender will be notified that the message was not delivered and why. The operations staff at RM keep records of all such undelivered mail and who the senders and intended recipients are

- **The prevention of "spam"** - Spam refers to all of the unsolicited junk e-mail that can clog up people's mailboxes once their addresses have been obtained from various sources. Our e-mail service is able to detect most spam messages by looking for certain key words and phrases which usually characterise them. If detected these spam messages are not delivered

- **The filtering out of computer viruses -** If a message contains a computer virus this will be detected by the e-mail system and the message will not be delivered. Both the sender and the intended recipient will be automatically informed of what has happened

Sensible Precautions

Nevertheless, there are still some basic precautions which pupils should always take.

- Whole-class or group e-mail addresses are used throughout the school
- Pupils should only send e-mail to people - whether they know them or not - who have been approved by their teacher
- All messages sent should be polite and responsible
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication
- Pupils must immediately tell a teacher if they receive offensive or unpleasant e-mail
- Pupils may only use approved e-mail accounts on the school system
- Social e-mail use is not allowed
- E-mail 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
- The forwarding of chain letters is not allowed
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts may be blocked

.

How is content on our school website managed?

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information must not be published
- E-mail addresses should be published carefully, to avoid spam harvesting
- The Headteacher has overall editorial responsibility and ensures that content is accurate and appropriate
- The website should comply with guidelines for publications including respect for intellectual property rights and copyright. The website is reviewed by the Governor in charge of the website

Publication of Images of Children on the school website

The school follows DfE guidelines for using images of children, including parents being asked to complete a form detailing their wishes. See Policy for Using Images of Children. This list is updated every year and a list is kept in the office.

How is social networking and personal publishing managed?

- The school blocks/filters access to social networking sites
- 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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, and e-mail addresses, full names of friends, specific interests and clubs etc
- Staff should be aware that bullying can take place through social networking [especially when a space has been setup without a password and others are invited to see the bully's comments] out of school and the problems associated with this can come into school

How are emerging technologies managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Pupil mobile phones are only allowed in school if a consent form is signed and agreed by the Head Teacher. The mobile will be kept in the office during the day.

How is personal data protected?

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998. The school follows the current GDPR recommended guidelines.

How is Internet access authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications
- All staff must follow the 'Staff Information Systems Code of Conduct' before using any school ICT resource
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials
- Parents are informed that pupils will be provided with supervised Internet access and are asked to sign and return a consent form for pupil access

How are risks 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 CSF can accept liability for the material accessed, or any consequences resulting from Internet use
- The school audits ICT use to establish if this 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
- Methods to identify, assess and minimise risks will be reviewed regularly

How are E-safety complaints handled?

- Complaints of Internet misuse will be dealt with by the Head teacher or by the ICT Subject Leader/Assistant Head teacher Mr McDonough.
- Any complaint about staff misuse must be referred to the Head teacher
- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will need to work in partnership with staff to resolve issues
- The school will follow the procedures and advice of Herts Grid for Learning
- Actions within the school are linked to the school's behaviour policy
    - discussion with Head teacher
    - informing parents and carers
    - Removal of Internet or computer access for a period

The Internet across the community

- The school liaises with Herts for Learning to establish and maintain a common approach to E-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice based on the recommendations of Herts for Learning.

How is the policy introduced to pupils?

- E-Safety Rules are explained and discussed with all classes by classteachers at a level appropriate to the age of the children. These are refreshed regularly with classes, groups, individuals as appropriate.
- E-Safety rules are posted near all computers with Internet access.
- Children in KS2 complete the Pupils' Agreement of the Responsible Internet Use Form.
- Pupils are informed that network and Internet use will be monitored.

How is the policy discussed with staff?

- All staff will be given the School E-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Day-to-day monitoring is carried out and advice provided by the ICT Subject Leader. Issues requiring more advice will be discussed with HfL and/or IntermIT
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required

How is parental support enlisted?

- Parents’ attention will be drawn to the school’s E-Safety Policy in newsletters, the school prospectus and on the school website
- Internet issues will be handled sensitively, and parents will be advised accordingly
- A partnership approach with parents will be encouraged
- Parental advice provided by Herts for Learning is distributed to parents.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents
- Interested parents will be referred to organisations listed in the E-Safety Contacts and References section at the end of this policy

E-Safety Contacts and References

Herts Grid for Learning – www.thegrid.org.uk

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta
http://www.becta.org.uk/schools/esafety

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog

Schools ICT Security Policy
http://www.eiskent.co.uk (broadband link)

Stop Text Bully
www.stoptextbully.com

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

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

E-Safety – The Legal Framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- ⊙ The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- ⊙ The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- ⊙ The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else’s password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission.

The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.