Barleyhurst Park Primary School

Barleyhurst Park Primary School

Core e-safety and acceptable use of ICT

Approved by Governors

Date: 18th July 2019

Signed: James Armstrong Chair of Governors

Barleyhurst Park Primary School

Contents:

Barleyhurst Park Primary School

What is e-safety?

- e-safety covers issues relating to children as well as adults and their safe use of the internet, mobile devices and other electronic communication devices. It includes education for all members of the school community on risks and responsibilities and is part of the school's duty of care.
- Our school e-safety policy has been written by the school, building on government and local authority guidance and other local school's e-safety policies.
- The e-safety policy relates to other policies including those for Computing, Anti-bullying, Child Protection and Safeguarding, Data Protection.

1. Introduction

Information Communication Technology in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including: web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites/internet
- E-mail, instant messaging and chat rooms
- Social media, including Facebook and Twitter
- Mobile/smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning platforms and virtual learning environments
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements, usually 13 years old.

At Barleyhurst Park Primary, we understand the responsibility to educate our pupils on e-safety issues: teaching them the appropriate behaviours and critical thinking skills needed to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual.

The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

2. Roles and responsibilities

As e-safety is an important aspect of the strategic leadership within the school the Headteacher and Governors have ultimate responsibility to ensure the policy and practices are embedded and monitored. The Computing Subject Leader is the e-safety coordinator and has been designated this role as a member of the senior leadership team. All members of the school community are aware of who holds the post. This role may also be covered by the Designated Child Protection Officer as the roles overlap. It is not a technical role.

This policy, supported by the school's Staff Code of Conduct for Computing, and the policy on Social Networking Sites and Personal Internet Presence for School Staff, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding, Health and Safety, Behaviour (including the Anti-Bullying) and PSHE.

3. e-safety in the curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- The school provides opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information and protecting their own personal information, safe use of images and other important areas through discussion, modelling and appropriate activities.
- Pupils are aware of the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies e.g. parent/carer, teacher/trusted member of staff or an organisation such as Cybermentors, ChildLine and Child Exploitation and Online Protection command (CEOP) report abuse button.
- Pupils are taught to evaluate materials critically and learn good searching skills through cross-curricular teacher models, discussion and via the computing curriculum.

4. Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

5. e-mail (applicable to staff and pupils)

The use of e-mail within the school is an essential means of communication. In the context of school, e-mail should not be considered private. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette: 'netiquette'.

- All e-mails should be checked carefully before sending, in the same way as a letter written on school headed paper. Staff work e-mails shall be sent via the school e-mail address.
- E-mails created or received as part of a staff member's school job are subject to disclosure in response to a request for individual information under the Freedom of Information Act 2000.
- Sensitive and/or pupil information should only be sent via the school e-mail system.
- Staff must inform the e-Safety Co-ordinator or Headteacher if they receive an offensive e-mail, whether it is directed at themselves or others, before it is deleted.
  The forwarding of chain letters is not permitted in school.
- Pupils may only use school approved accounts on the school system for educational purposes and only under direct teacher supervision.
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments. E-mails must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, e-mails should not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail whether directed at themselves or others and before it is deleted.
- Pupils are introduced to e-mail as part of the computing curriculum in Year 2.
- However school e-mail is accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending e-mails

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possibly, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising.

Receiving e-mails

- Check e-mail regularly,
- Never open e-mails or attachments from an untrusted source; consult the ICT lead first if in doubt.
- Do not use the e-mail system to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

6. e-safety support for staff

Staff receive regular and appropriate information and training on e-safety and how they can promote the 'Stay Safe Online' messages. This is usually through the scheduled programme of staff meetings.

New staff receive information on the school's acceptable usage policy as part of their induction.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

7. The internet

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and whenever any inappropriate use is detected it will be followed up.

- The school provides pupils with supervised access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- On-line gambling or similar activities are not allowed.
- All staff, volunteers and governors must comply with the policy on Social Networking and Personal Internet Presence for School Staff regarding the posting of any information or images relating to the school.
- School internet access is controlled through the LA's web filtering service via E2BN.
- Barleyhurst Park Primary School is aware of its responsibilities when monitoring staff communication under current legislation.
- Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-Safety Co-ordinator or teacher as appropriate.
- It is the responsibility of the school to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Computing Subject Leader.
- If there are any issues related to viruses or anti-virus software, the Computing Subject Leader should be informed.
- The school does not allow any access to social networking sites.
- Staff or pupil personal information will not be published on the school website. Any contact details online should be those of the school office.

- After permission has been obtained from parents or carers, pupil photographs/work may be published on the school website or blog. Pupil image file names will not refer to the pupil by name.
- With regard to the school's website, the Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

8. Taking of images and film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

- Staff and visitors are not permitted to use **personal** digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. Appropriate images can be taken using school cameras; these should be transferred as soon as possible to the school's network and deleted from the individual device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.
- Staff must have permission from the Headteacher before any images can be uploaded for publication.
- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.

9. Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/transmitted on a video or webcam.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their images and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting a child's work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed.

10. Storage of images

- Images/films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media (e.g. USB sticks) for storage of images without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resources.

11. Web cams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specified learning purposes and our pupils' use of webcam is appropriately supervised for the pupil's age.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document). Staff must ensure webcams are switched off when not in use.

12. Video conferencing

- Permission is sought from parents and carers if their children are involved in video conferences.
- All pupils are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school
- No part of any video conference is recorded in any medium without the written consent of those taking part.
- Video conferencing should use the educational broadband network to ensure quality of service and security

13. Personal mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device. The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.
- The creation of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Pupils' mobile phones and/or personal devices are to be handed into the school office and are not permitted for use during the school day.
- All staff sign the school's code of conduct regarding mobile phone use.

14. Learning platforms.

- The Computing Subject Leader and staff will regularly monitor the usage of the Virtual Learning Platform (VLE) by pupils and staff, in particular monitoring messaging and communication tools.
- Pupils and staff are advised about acceptable conduct and use when using the VLE and how to report any concerns of misuse.
- Only members of the current school community have access to the VLE.

15. Cyber-bullying

- Cyber-bullying is defined as, 'The use of ICT, particularly mobile phones and the internet, to deliberately hurt or upset someone' DCSF 2007.
- Cyber-bullying (along with other forms of bullying) of any member of the school community will not be tolerated.
- All incidents of cyber-bullying reported to the school will be investigated and recorded, in line with the school's anti-bullying policy.

16. Parental involvement

- Parents/carers are asked to read through and sign the Responsible Use Parent/Child Agreement with, and on behalf of their child on admission to the school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website).

17. Security

The school gives relevant staff access to its Management Information System, with a unique username and password.

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others.
- Staff are aware of their responsibility when accessing school data.
- Staff are issued with the relevant guidance documents and the Staff Code of Conduct for ICT document.
- Staff keep all school related data secure. This includes personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile computing equipment or removable storage media in unattended vehicles. Where this is not possible, it should be kept locked out of sight.
- Staff should always carry portable and mobile computing equipment or removable media as hand luggage, and keep it under their control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

- All computing equipment is security marked as soon as possible after it is received. The Office Administrator maintains a register of all computing equipment and other portable assets.
- As a user of the school computing equipment, you are responsible for your activity.
- Computing equipment issued to staff is logged and serial numbers are recorded as part of the school's asset register.
- It is imperative that staff save data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any of your data that is not held on the school's network.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned computing equipment should not be used on a school network.
- Staff should not use any 3G/4G internet access on mobile devices to bypass school filtering systems.
- On termination of employment, registration or transfer, staff must return all computing equipment to the school. Staff must also provide details of their system log-on so they can be disabled.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- The installation of any applications or software packages must be authorised by the Computing Subject Leader or the Headteacher.
- Portable equipment must be transported in its protective bag.

Server security

- School servers are kept in a locked and secure environment and there are limited access rights to these.
- Existing servers have security software installed appropriate to the machine's specification and the school uses a remote back up service and data is backed up daily.

Using removable media

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by the computing support team.

Monitoring

- Both this policy and the Staff Code of Conduct for ICT are inclusive of both fixed and mobile internet; technologies provided by the school (such as PC's, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).
- Internet activity is logged by the school's internet provider and in addition the school's technicians regularly monitor the websites which are accessed on school equipment.

17. Breaches

- A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school computing hardware, software or services from the offending individual.

- Any policy breach is grounds for disciplinary action in accordance with the school policy; breaches may also lead to criminal or civil proceedings.

19. Incident reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of computing must be immediately reported to the school's E-Safety Co-ordinator and/or Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access secure ID tokens and PINs), virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

An incident log is used to monitor what is happening and identify trends or specific concerns. The log is kept in the school office.

- All users are aware of the procedures for reporting accidental access to inappropriate material. The breach must be immediately reported to the E-Safety Co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident begin logged by the E-Safety Co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, possibly leading to disciplinary actions, dismissal and involvement of police for very serious offences.
- Complaints/concerns of a child protection nature must be dealt with in accordance to the school's child protection procedures.

20. Protecting personal, sensitive, confidential and classified information

Staff will ensure:

- They lock their screen before moving away from their computer during the normal working day to prevent unauthorised access.
- Personal, sensitive, confidential and classified information is not disclosed to any unauthorised person.
- The security of any personal, sensitive, confidential and classified information contained in documents which are faxed, copied, scanned or printed.
- Only download personal data from systems if expressly authorised to do so by the Headteacher.
- They keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.
- Hard copies of data are securely stored and disposed of after use in accordance with the document labelling.
- They protect school information and data at all times, including any printed material.

21. Viruses

- All files downloaded from the internet, received via e-mail or on a removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school computing equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your computing team.

- If you suspect there may be a virus on any school computing equipment, stop using the equipment and contact your computing support provider immediately. The computing support provider will advise you what actions to take and be responsible for advising others that need to know.

22. Disposal of computing equipment

- All redundant computing equipment will be disposed of through an authorised agency recommended by the LA. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Any redundant computing equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and, if personal data is likely to be held, the storage media will be overwritten multiple times to ensure the data is irretrievably destroyed.
- All redundant computing equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.
- Disposal of any computing equipment will conform to current legislation and will conform to the governors' policy on the disposal of equipment.

23. Zombie accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Technical staff will ensure that all user accounts are disabled once the member of staff has left the school.