Keir Hardie Primary School & Children's Centre

Online Safety Policy

Reviewed:	**Summer 2018**
Date of Next Review:	**Autumn 2019**

Online Safety Policy

This policy was reviewed by the co-ordinator

Print Name ……..

Signature …….

Date ……

This policy was reviewed by the Head Teacher

Print Name ……..

Signature …….

Date ……

This policy was reviewed and agreed by the Chair of Governors

Print Name ……..

Signature …….

Date ……

Acceptable Use & Internet Safety Policy

Being online is an essential part of life and education in the 21st century. The main purpose of the Internet at Keir Hardie Primary School[1] is to prepare children for the future and to raise educational standards. We seek to provide pupils with quality Internet access as part of their learning experience. The Internet is an integral part of everyday life; therefore this policy provides a framework for the safe and appropriate use of the Internet for all members of the school community.

Aims and objectives

Through safe use of the internet we aim to:

- understand computer networks including the internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for communication and collaboration
- Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information

Guidelines

1. Pupil's online access

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Responsible usage of the Internet for all pupils should be taught routinely through Computing – especially with J2e and Google and the benefits to working collaboratively and being able to access a document anywhere in the world. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "What is the purpose?

Children will be taught use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Sharing websites via J2e and Google are a useful way to present this choice to pupils.

2. Filters

Keir Hardie Primary School has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network. We use the LGfL filtering system which blocks sites that fall into categories such as

[1] Please note: 'School' refers to KH Primary School and KH Children's Centre

pornography, race hatred, gaming, sites of an illegal nature, and prevents access to extremist websites and materials etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status. We USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students. Our SBT (school based technician) ensures the network is healthy through use of Sophos anti-virus software (from LGfL) etc and the network is set-up so staff and pupils cannot download executable files. All chat rooms and social networking sites are blocked except those that are part of an educational network or approved Learning Platform. Any sites which the school wants unblocking needs authorising through the head teacher, and written confirmation needs to be sent to Tania Hebel at ITASS.

3. Online-Safety

All teachers are responsible for promoting and supporting safe behaviour in their classroom and following school Online-Safety procedures. Central to this is fostering a 'No Blame' culture where pupils feel able to report any bullying, abuse or inappropriate materials. Children will receive Online-Safety education once an academic year, to teach them the importance of being safe online and highlighting the potential dangers that they can be exposed to.

Online-safety is taught in every year group. EYFS use Smartie the Penguin, Key Stage One: Hectors World, Key Stage Two: Cyberpass – a new LGFL resource, which assesses children's needs and provides a whole range of resources covering settings, privacy, looking, sharing, playing, talking and friendships on line. All stimuli is designed to pose problems that children can solve through real-life simulations.

Social Networking Sites - These are a popular aspect online for young people. Sites such as: Facebook, Instagram, Snapchat, WhatsApp and YouTube allow users to share information and communicate with each other. It is important for children to understand that most social networking sites carry an age restriction of 13 and that this space is used by the vast majority of the population; these are environments that should be used with caution.

Prevent Duty

As a school we aim to ensure that children are safe from terrorist and extremist material when accessing online at school. As outlined above, suitable filtering is in place to protect pupils. All teachers are aware of the risks posed by the online activity of extremist and terrorist groups, and by communication with parents and sharing guidance on safe internet access at home and supervision by an adult, we aim to ensure that pupils are protected from the threat of radicalisation. In the case of any member of staff or pupil attempting to access inappropriate material online, the school would make a referral to the Channel programme in accordance with government and Local Authority guidelines, See the school's Prevent Duty Document.

Pupils:

We use J2e and Google with the pupils and lock this down where appropriate using LGfL filtering. Pupils' USO and Google accounts are not visible to others and handed out to that person only. Pupils are introduced to the cloud and working collaboratively on

a document and communicating online as part of the Computing scheme of work. Pupils are taught about the safety of communicating online both in school and at home i.e. they are taught:

- not to give out their username and password unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- they must not reveal private details of themselves or others in an online, such as an address, telephone number, etc;
- to 'Stop and Think Before They Click' and not to open a link unless they are sure the source is safe;
- that they should think carefully before uploading any attachments as this will remain online forever;
- that they must immediately tell a teacher / responsible adult if they receive a document online which makes them feel uncomfortable, is offensive or of a bullying nature;
- not to respond to malicious or threatening messages.

4. Use of email

We do not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@keirhardie for communication with the wider public. The school will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law. The school manages accounts effectively with up to date account details of users. We are aware that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

5. Web-publishing

The school has its own website, and the school is registered under the Data Protection Act. Parental consent is gained upon admission to the school. This is required before any text, audio, pictorial or photographic reference to a child or children being published. Records are kept of parents or carers who decline permission. Individual pupils will not be identifiable by name, and names will not be linked to any photographs. Personal information will never be published without prior consent.

6. Reporting incidents

If one or more pupils discover (view) inappropriate material, the first priority is to provide them with support. Children should report any unsuitable sites to the class teacher. The class teacher is then responsible to report the inappropriate material to the Computing co-ordiator. From there the Computing co-ordiantor should inform the head teacher and LEA in order to get the sites blocked. Due to the upgraded LGFL filters there are a lot more restrictions placed upon the internet.

Incidents which occur due to non-compliance with the school Online-Safety policy should be reported to the Online-Safety co-ordinator (Violet Otieno) issues relating to staff misuse must be referred to the head teacher. Any incidents which refer to children protection must be reported to either Jean Bond or Violet Otieno.

7. Parents and the community

Pupils' online access at home is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy. Parents' attention will be drawn to the school Online–Safety Policy in newsletters, the school prospectus and on the school website.

8. Roles and responsibilities

Online-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online-Safety has been designated to a member of the senior management team.

Our school Online-Safety Co-ordinator is Georgie Eastman.

Our Online-Safety Co-ordinator ensures that she is up to date with Online-Safety issues and guidance through the Local Authority Online-Safety Officer and through organizations such as Becta, LGFL, NSPCC and CEOP. The school's Online-Safety Co-ordinator ensures the Head, senior management and the Governors are updated as necessary.

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- NPW (Newham Partnership Working) will appoint a Data Protection Officer (DPO) with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners in a spreadsheet.
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record on Google Docs

  We ensure ALL the following school stakeholders are sent an Acceptable Use Agreement (updated April 2018)

This makes clear all responsibilities and expectations with regard to data security.

- We have approved educational web filtering across our wired and wireless networks.
  We monitor school <e-mails / blogs / online platforms, etc.> to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- Staff use Fronter (MLE) to access school data remotely when not at school. This is password protected. USB devices must not be used to transfer school data from school computers.
- School staff who set up usernames and passwords for e-mail, network access, or other online services work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We will shortly be introducing a no-flash drive/USB memory stick rule for transferring personal data from school computers to external computers. All data will have to be accessed via the remote password-protected systems listed below.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins. idle time. Curriculum computers are set to automatically turn off at 6:30pm.
- We use RAV 3 for remote access into our systems.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use the Pan-London Admissions system to transfer admissions data. Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use LGfL AutoUpdate for creation of online user accounts for access to services and online resources.
- We use LGfL's USO-FX2 to transfer documents to schools in London, such as references, reports of children.
- We use MyUSO accounts for online document storage.

- We store any sensitive/special category written material in lockable storage cabinets in a locked room
- All servers are in lockable locations and managed by DBS-checked staff.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our network / admin, curriculum server(s).
- For ICT disposal, we delete all data from hard drives and memory and dispose of the equipment via Newham Council
- Portable equipment loaned by the school for use by staff at home, where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded.

Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely. As part of the LGFL filtering these sites are blocked within school, however as a duty of care to both students and adults it is our responsibility to educate about the potential dangers.