Stroud Green Primary School

Believe and achieve

Stroud Green Primary School, part of a richly diverse community, is a place where all children flourish in a safe, happy and stimulating environment.

E-Safety Policy

Reviewed at Curriculum Committee: Spring 2016

Date of next review: Summer 2018

The e-safety officer for the school is the Head teacher.

Our e-safety policy recognises that measures must be in place in order to ensure technology is used safely within all areas of learning and teaching. All reasonable steps are taken in order to safeguard our children and ourselves.

Virus Protection:

Only software with a site-licence that has been purchased by the school or the Local Authority is allowed to be used on the school premises.

Pupils are not allowed to bring private software disks or removable storage devices into school and, in particular “arcade” games software is banned. If found in school they will be confiscated and sent to the ICT manager, who will scan them for viruses and check if any breach of copyright has been made. In such cases, the ICT manager will report to the head who will decide on the appropriate action to be taken. If children bring in CD Roms relating to their work, these will be used at the teacher’s discretion.

Staff using removable storage devices must ensure that their home PC / laptop has adequate virus protection (regularly updated and scanned) to safeguard the school network when transferring data. If a virus has been detected on external PC systems then the removable storage devices MUST not be used within the school. Emailing files to school from a system with a known virus can seriously damage the school network and must not be carried out in any circumstances.

Pupils who need to bring in work from home systems should email (with staff permission) as they are not permitted to bring in any removable storage devices.

Virus protection software is installed on all networked computers. This software will be updated regularly according to the procedures set by the technician who will check that this has been completed. LA advice to protect the school from specific viruses will be taken. Staff (using laptops on home ISP) need to ensure that laptops are updated and scanned regularly and must notify the technician if a virus has been detected.

Staff must take every precaution to ensure the safety of school systems, their own pcs and laptops with regard to virus protection and internet security.

Unauthorised Access:

All personal, confidential and sensitive information will be protected by password restricted to authorised personnel only and will only be stored on a removable storage device if it is absolutely essential. When a removable storage device does contain confidential data, it will be stored in a locked safe or secure area.

Software Router: LgFL

- Web guards protect the children from banned and unacceptable web sites.
- Lists of banned sites will be updated as appropriate.
- The router shall be securely locked away.
- Logging in passwords and other codes should not be divulged to the pupils.
- Pupils should not have access to logging in codes or other information related to the school systems.

Protecting Pupils from on line risks:

Introducing children to positive use of technology at an early age is important to ensure that they remain safe and aware of potential dangers and correct use of modern technology. Over the course of their learning within the school, teachers ensure that all age appropriate aspects of e- safety are covered with the pupils. Lessons around e-safety are explicitly delivered. Pupils learn about safe use of a range of modern technologies and as new advice is circulated from the LEA relevant year groups will be updated.

No pupil of any age is allowed access to the computing suite or any other networked computer at any time, unless they are under the supervision of a member of staff. This is because of the internet connection available on all of the computers and our duty to protect the pupils at all times. Any staff discovering unsupervised pupils in the ICT suite accessing any school computer must evict them and they must return to their class teacher.

Younger children who are using a specific site chosen and accessed by a member of staff must be restricted to that site and be directly supervised to ensure that they do not access other information on the internet.

Staff must ensure that class computers and laptops are either shut down or in a safe mode when left during break times.

The pupils must be aware of the following points, before they are allowed to access the Internet:

- The rules for safe surfing and internet access, STOP, THINK, GO procedure, which teachers will remind them of frequently.
- That there are inappropriate sites on the Internet.
- That some sites may have ‘pop ups’ which contain links to inappropriate material and they must follow the internet safety code.
- We inform parents if pupils deliberately try to access inappropriate sites.
- Pupils may not communicate directly with others over the Internet (unless requested to do so by a teacher as part of the curriculum), but may request information through a member of staff.
- That games and fun sites may only be accessed with the express permission of the member of staff.
- Pupils may not reveal their location or any other personal information by entering it in any form. They must ask a member of staff about any site requesting personal details.
- Permission must first be obtained from staff to download and print off any information. Pupils will be informed about plagiarism and copyright theft.
- That pupils may access inappropriate sites by mistake, or they may read something inappropriate, racist, cruel or in any other way upsetting.
- Pupils must be informed that receiving and sending unkind, racist and other derogatory comments through messaging systems (blogs/ web space) is called cyberbullying and will be dealt with in line with our discriminatory incidents policy
- If any inappropriate material is accessed on a school computer the pupils must cover or switch off the screen and immediately alert the member of staff in the computer suite. Failure to do so immediately will result in those pupils being

restricted from using the computer suite. The teacher must inform the Head teacher who will decide if further action is necessary.

- Similarly, If staff access any inappropriate internet sites during the course of their research they must inform the Head teacher. Staff need to be aware that visiting websites leaves cookies on the computers which means evidence of the websites they have visited are contained on the computers.

Chat rooms, Blogs and Personal Webspace:

Pupils should be made aware of the rules for safe usage. Older pupils should gain a greater understanding of associated dangers and safe secure methods and sites. Pupils should understand how to remain safe and secure when setting up and using these technologies. Pupils should be informed that viewing and posting of inappropriate and unkind comments on a Blog/ web site is unacceptable and is called cyber bullying. It will be dealt with following the school's behaviour policy.

Staff should not share personal email addresses with pupils. Children needing to send emails to staff should forward emails via the school administrator at admin@stroudgreen.haringey.sch.uk

All e-safety rules that relate to the computer suite also relate to ipads. All school ipads are kept ina lockable cupboard and staff must sign out when suing the ipdas with children.

Cameras and iPads

We recognise that one of the key ways that staff support children's development and engage parents in children's learning is through photographs that record their activities and achievements. However, it is essential that photographs and videos are taken and stored appropriately to safeguard the children in our care.

We will:

- Check with parents that they consent to the use of cameras for appropriate recording purposes.
- Only use designated school cameras to take photos or videos in school or on outings.
- Ensure images taken are suitable without putting children in any compromising positions that could cause embarrassment or distress e.g. photographs should not be taken in bathroom areas.
- All staff are responsible for the location of cameras, which are to be stored securely when not in use.
- Images taken and stored on the camera must be downloaded as soon as possible, ideally once a week.
- If the technology is available images should be downloaded on-site. Should this facilities not be available these may be downloaded off-site and erased from the personal computer as soon as practicable.

Mobile Phones:

So that staff and children are not being distracted from their work and in order to prevent theft and the inappropriate use of mobile phone cameras around children, we adhere to the following:

- Families must request permission if they want older pupils to bring mobiles into school. If given permission, they must hand mobiles into the office on arrival and collect their devices at the end of the day.
- Staff may bring personal mobiles and devices to school for their own use but must ensure there is no inappropriate or illegal content on them.
- Staff must not contact pupils or their families using their personal device.
- Staff must not access mobiles/devices during contact time with children, unless it is part of an agreed safety plan. They should be stored securely.
- Mobile phone calls may only be taken at staff breaks or in staff members' own time and in an appropriate place.
- If a staff member has a family emergency and needs to keep their mobile phone to hand, prior permission must be sought from the Headteacher.
- During outings nominated staff can use a mobile devices, for emergency purposes or to inform school of updates.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher.
- Concerns will be logged and investigated appropriately (see allegations against a member of staff policy).
- The Headteacher or her deputy in her absence reserves the right to check the image contents of a mobile phone should there be any cause for concern over the appropriate use of it.
- Should inappropriate material be found then our Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO as to the appropriate measures that are the required.