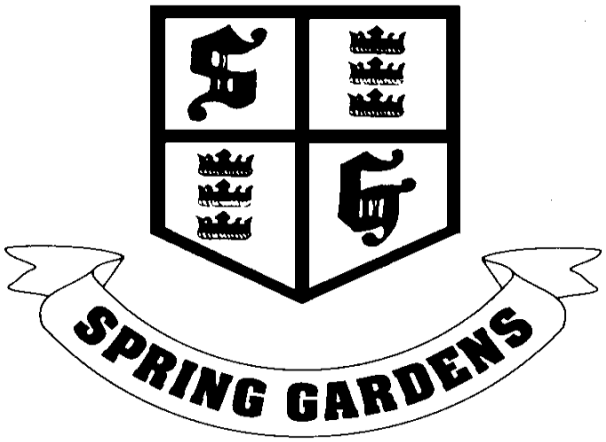
Spring Gardens Primary School



Policy for e-safety

Reviewed: July 2017

1. Introduction

Pupils interact with the internet and other communications technologies such as mobile phones on a daily basis. The exchange of ideas and social interaction are both greatly beneficial but can occasionally place young people in danger. E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones and other technologies, both in and out of school. Spring Gardens Primary School takes these risks seriously and all emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

2. Aims

- To ensure all pupils and staff have a framework to work from with regards to e-safety.
- To protect the children in Spring Gardens Primary School from potential risk and harm.
- To educate children in the correct use of these technologies and how to report anything they deem as undesirable.
- To ensure the school has procedures for reporting and dealing with breaches to e-safety.

3. Teaching and Learning

3.1 Why the Internet and emerging technologies are important.

- The Internet and many emerging technologies are an essential element to life in the 21st century. They are essential to education, business and social interaction. Our school has a duty to provide its pupils with quality internet access as part of their learning experience and the ability to use new technologies for educational reasons.
- Internet use is a part of the statutory curriculum and a necessary tool for both pupils and teachers.

4. Managing Internet Access

4.1 Internet Access

- Pupils should not access the internet unless supervised.
- Staff will be allowed to use the internet for their own use as long as it is not used in teaching time and the access does not breach the e-safety policy.

4.2 Internet content

- All internet content will be filtered by the North Tyneside filtering system.
- If staff or pupils do discover unsuitable material the e-safety co-ordinator (head teacher) should be notified. The URL should be noted and the site investigated. If the site is visited as an investigation the time and date of that access should be noted and the reason for accessing the site given.
- The use of search engines can be dangerous and should be monitored at all times. Example search terms should be provided prior to research.
- Google image search should be avoided. When possible teachers should search for appropriate pictures and save them in a shared area of the network. This not only

decreases the risk involved but also maximises teaching time. Microsoft clipart is a good searchable resource for digital media.
- Logs of all internet access will be reviewed on a regular basis by the head teacher.

4.3 E-mail

- The school uses gmail through the NTLP (North Tyneside Learning Platform. All staff have their own e mail address and children have their own email address (given in Year 3 as part of the ICT topic)
- Children will be educated on the rules of using their NTLP email account.
- Teachers should be aware that their e mail accounts are not private and can be monitored.
- The school will add a standard disclaimer to all emails.
- Children are not allowed to access any other web based e-mail systems within school, for example: Hotmail.
- Staff are only permitted to use their NTLP and .gov account on the school network.
- Children should be taught how to create safe and secure passwords.

4.4 Social networking and personal publishing

- Access to all social networking sites (networking sites such as Facebook, Instagram, chat rooms, instant messaging, blogs, newsgroups) will be blocked using filtering systems.
- Pupils will be made aware that they should not publish any personal information on any website either in school or at home or arrange to meet anyone.
- Pupils and parents should be made aware of the age restrictions associated with the various social media networks.
- The children should be made aware of how to report any behaviour including online bullying which they feel is inappropriate.
- Parents should be made aware of the dangers of these sites and regular information and workshops will be arranged by the school. These meetings will be resourced by LEA staff.
- All staff have a duty to deliver regular e-safety lessons and discussions to keep children up to date and aware of staying safe online.

4.5 School Website

- No contact details of pupils or staff will be included on the school website. Contact details will be the school address, e-mail and telephone number.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

5. Network Security and confidentiality

5.1 Network security

- School ICT systems capacity and security will be reviewed regularly.
- The network operating system should be kept fully up to date with all appropriate updates and patches installed (this is the responsibility of the network manager).
- Only the network manager should install programs onto the network. Users should not download programs or install software without permission. The network security is set up so that this cannot happen inadvertently.

- Classes with iPads sets should teach children how to use these in line with the school policy. A signed responsible use agreement should also be returned to school before children are permitted to take the iPad home.
- Children taking an iPad home may join their home network in order to access online homework apps (e.g. Mathletics or Spellodrome) but may not download any apps or make changes to the iPad settings.
- Teachers have an allocated laptop. These are taken home. The use of these laptops at home must comply with the e-safety policy. When outside of school these laptops should only be used by the allocated teacher.

5.2 Antivirus

- The network has antivirus protection on the server and all workstations.
- The virus definitions are kept up to date and a regular virus scan should be carried out on laptops. The virus checker also provides real time virus protection for internet access.
- Pupils are not allowed to use any removable media on the network (flash memory, floppy disks)

5.3 Confidentiality

- No user of the network should access other users work areas or files without the express permission of that user.

5.4 General network use

- Teachers should keep their areas of the network organised and delete or write to USB (especially videos and images) that are not necessary. Storage should not be backed up to laptop hard-drives and the shared area school network. Teachers should ask colleagues for support with this if necessary.

6. Digital images and video

6.1 Parental pictures and video

- The school will seek permission from parents/guardians to allow pupils to be photographed. Any children without permission will not be included. Parents are reminded to keep any photos taken during whole school events for personal use and under no circumstances are images to be used on social media.

6.2 School pictures and videos

- The school may use photographs and videos of the children for curriculum use without permission from parents/guardians.
- The school will seek permission from parents/guardians before photographs are used for display purposes, publication on the school web site or publication in local or national press.
- Any pictures or videos of children should be stored on the staff area of the school network. Once on the school network the images should immediately be deleted from the device.
- Teachers should be careful not to take devices with images of children stored on them home.

6.3 Parental permission procedures

- Parents/guardians will be given a photograph agreement form when their child first joins the school. This form will seek permission for:
    - The use of photographs in displays.
    - The publication of photographs on the school website or in the press.
    - Allowing other people associated with the school, for example, parents to photograph events involving their children.
- This permission will be applicable for the duration of that child's time at Spring Gardens, unless the school is informed otherwise.

7. Mobile phones

7.1 Children's phones

- No use of mobile phones by children is permitted within school unless in an emergency and under supervision.
- All phones brought into school by pupils are handed in and kept in a secure place within the school office. This cuts down on risks of theft, texting and phoning etc.
- Staff need to be aware of issues relating to cyber bullying that can occur out of school and how to deal with issues which are brought into school.
- If children do feel they are suffering from cyber bullying they should report this to their parents/carers or a teacher. Any persistent or long term incidents should be logged in accordance with the school's anti-bullying policy.

7.2 Staff phones

- Staff phones are permitted in school but should only be used for personal communication in non-teaching time.
- Staff must not pictures on a mobile phone.

8. E-safety complaints or non-compliance with policy

- All incidents of e-safety incidents or non-compliance to the policy should be recorded on CPOMS and shared with appropriate members of the pastoral/senior leadership members.
- Any inappropriate websites visited by the staff or children should be logged with their URL for further investigation. If these sites are investigated the URL and date of the investigative visit should be logged.
- All incidents should be reported to the head teacher.
- Inappropriate use of technology will be dealt with according to the situation.
- Parents may be informed if the situation is deemed serious enough.
- Potential child protection or illegal incidents must be reported to the head teacher where appropriate steps will be taken.

9. How are stakeholders informed of this policy?

Staff

- This policy is written in consultation with the teaching staff. Staff are given a copy of the policy with time to discuss its implications to their teaching.

Children

- Children will be given an acceptable use policy for e-safety. This policy will include the points relevant to children and will be in child friendly language.
- E-safety posters will be put up around school and near every workstation to remind pupils of basic e-safety considerations.
- Children will be educated in age relevant aspects of e-safety throughout the school.
- Every child in every class will sign an 'acceptable use' poster, which will help focus discussions regarding online safety.

Governors

- The draft policy is taken to the school governing body. The governors are given the opportunity to discuss the policy and its implications. This policy must be ratified by governors.

Parents

- This policy will be available for parents to view via the school website.
- Parents will be made aware of aspects relevant to them, for example, consent for images etc via letters from school.
- The school will continue to inform parents of the dangers associated with e-safety.

10. Review of policy

- This policy will be reviewed annually in most cases.
- The policy may be reviewed in the light of incidents occurring in or out of school or with the emergence of new technology.
- The policy will be reviewed in child-friendly language by the school council, to ensure that it is kept up to date with new devices, apps and media networks.