Pol No:51
Statutory
Review date: Spring 2019

Park Mead Primary School

Park Mead Primary School E-Safety Policy

Park Mead School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Writing and reviewing the e-safety policy

E-safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, data handling and the use of images.

Using this policy

- The school will form an e-safety committee and will appoint an e-safety coordinator. (See Appendix 1 for the role of e-safety coordinator).
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Teaching and learning

Why Internet and digital communications are important

- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Park Mead Primary School

Pupils will be taught about online safety as part of the curriculum.
In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system, which is checked and monitored weekly to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the Internet via school equipment for anyone not employed by the school is filtered and monitored.

Managing Internet use

The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Any, and all, communication between staff and pupils or families will take place using school equipment and/or school accounts. Pupils will be advised not to give out personal details or information, which may identify them or their location.

E-mail

- **Staff may only use approved e-mail accounts on the school system.**
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher, office staff and Computing coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used on the web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. (See photographic permission policy P52 for further information).

Managing filtering

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- A filtering report is sent to the e-safety coordinator once a week showing any safeguarding triggers.
- Use of and communication on the 'Reading Cloud' online library will be monitored by teachers. Pupils reviews and comments must be approved by the class teacher before going online.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for the pupils' age

Park Mead Primary School

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.
- Memory cards from school digital cameras will be regularly formatted.

Use of personal devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the e-safety policy and the relevant Acceptable Use Policy (AUP).
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Handling and GDPR Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site and remote access to school systems.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and GDPR.

Cyber-Bullying

- Cyber-Bullying consists of: threats and intimidation sent to a pupil by mobile phone, email or online; harassment through repeated unwanted contact of another person; name calling online; public posting or forwarding of images without consent.
- Allegations of cyber-bullying will be handled in the same way as bullying (as seen in the anti-bullying policy).

Prevent Duty (July 2015 update)

- Suitable filtering and supervision should be in place in order to ensure children are kept safe from terrorist and extremist material when accessing the internet in school.
- Through e-safety and PSHEC lessons, pupils are to be equipped with the skills and knowledge necessary to stay safe from inappropriate material online, including terrorist and extremist material.
- Every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups and will have completed the prevent training (https://www.elearning.prevent.homeoffice. gov.uk/edu/screen1.html#) as part of the annual safeguarding training.
- Fundamental British Values are advertised and delivered to children on a regular and embedded basis, within the wider school curriculum.

Pol No:51
Statutory
Review date: Spring 2019

Park Mead Primary School

Policy Decisions

Authorising Internet access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.
- People not employed by the will be monitored by a member of staff when given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff according to the school's behaviour policy.
- Any complaint about staff misuse must be referred to the e-safety coordinator or head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the Internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

Introducing the e-safety policy to pupils

- Appropriate elements of the e-safety policy will be shared with pupils

Park Mead Primary School

- E-safety 'SMART' rules will be posted in all networked rooms and displayed in every classroom.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils

Staff and the e-safety policy

- All staff will be given the School e-safety Policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- All staff will receive e-safety training on a minimum annual basis.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on e-safety in the form of written communications or workshop type events.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child.

Policy review

- This policy will be reviewed annually and updated in line with DfE (Department for Educaton) or SSCB (Surrey Safeguarding Children's board) guidance or legislation.

Agreed by the Governing Body on…… Spring 2019……..

Next Review: Spring 2020 (Or as new guidance is released via SSCB or the DfE)

Signed by:…….

Chair of the Governing Body

Pol No:51
Statutory
Review date: Spring 2019

Park Mead Primary School

Appendix 1

The Role of the E-safety Co-ordinator.

- Complete an e-safety audit (in section 5.0 of this guidance) in conjunction with the Senior Leadership Team and/or Head

- Promote an e-safe culture under the direction of the management team, and promote the school's e-safety vision to all stakeholders

- Maintain the school's e-safety policy, reviewing annually

- Ensure that the e-safety policy links with other appropriate school policies e.g. Anti-Bullying, Child Protection, ICT, PSHE etc. (with the appropriate member of staff)

- Ensure the e-safety policy and its associated practices are adhered to (e.g. incident flow charts, reporting logs etc.)

- Ensure Acceptable Use Policies/school internet rules are in place, up-to-date and wherever possible are agreed by Staff, Pupils and Parents

- Work with the SENDCO and Designated Child Protection Officer to create e-safety guidance for vulnerable children and those with additional learning needs

- Manage e-safety training for all staff and ensure that e-safety is embedded within continuing professional development

- Ensure staff receive relevant information about emerging issues

- Coordinate e-safety awareness raising/education for pupils and ensure that e-safety is embedded in the curriculum, for example via e-safety schemes of work, assemblies and/or theme days

- Support e-safety awareness raising/education initiatives for parents

- Act as a point of contact, support and advice on e-safety issues for staff, pupils and parents

- Act as the first point of contact should an e-safety incident occur (particularly child protection or illegal issues), and ensure the agreed e-safety incident procedure is followed, as outlined in the school's e-safety policy

- Maintain an e-safety incident log in collaboration with the school's designated safeguarding lead

- Monitor, report and address incidences of pupils accessing unsuitable sites at school as necessary
- Keep up-to-date with local and national e-safety awareness campaigns and issues surrounding existing, new and emerging technologies

- Work with and receive support and advice from the SSCB e-safety sub-group and where necessary, the Policy.

Pol No:51
Statutory
Review date: Spring 2019

Park Mead Primary School

Appendix 2

Staff Template Acceptable Use Policy (AUP)

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the e-safety coordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that all electronic communications with parents, pupils and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Governing Body.
- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network/learning platform without the permission of the Head teacher.
- I will not install any hardware or software without the permission of the ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my performance manager or Head teacher.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the E-safety Coordinator, the Designated Safeguarding Lead or Head teacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

User Signature: I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Full Name ……
(Printed)

Job Title …….

Pol No:51
Statutory
Review date: Spring 2019

Park Mead Primary School

Signature…… Date……