Epsom Primary and Nursery School

E_SAFETY POLICY

Date of issue:	**January 2019**	**Owner:**	**Innovations Lead**
Date of review:	**January 2020**	**Governor Committee:**	**SLT**

Signed…….. Date……

Definition

We are keen to encourage children to be active learners who enjoy learning about technology in a safe environment. The aim of our e-safety policy is to ensure that technology used within school is safe to use and that children understand the risks of using technology to access, for example the internet. E-safety forms part of the school's safeguarding responsibilities and relates to other policies including those for **behaviour, safeguarding, anti-bullying, data handling and the use of images.**

Using this policy

- 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 and its implementation will be reviewed annually. The next review is due on: January 2020.
- 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.
- E-safety matters may also be referred to the Headteacher and/or DCPO as part of our safeguarding policy.

Physical Safety:

- All electrical equipment in the school is tested annually to ensure that it is safe to use. *Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum.* **We expect pupils to behave appropriately near electrical sockets and appliances.**
- All the projectors in our school have maximum light levels below the government's health and safety guidance of 1,500 ANSI lumens. *Pupils are taught that they should not look directly at strong light sources such as the sun, lasers or data projectors.* **We expect all users to not look directly into the light beam when working on the interactive whiteboards.**
- Workstations are cleaned and sanitised regularly. *Pupils are taught to avoid taking food and liquids anywhere near the computers.* **We expect all users to refrain from eating and drinking when working at a computer.**

- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. *Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy.* **We expect all users to take responsibility for their own physical well-being by adopting good practices.**

- Computers and other ICT equipment can be easily damaged. *Pupils are taught the correct way to use ICT equipment.* **We expect pupils to respect ICT equipment and take care when handling and using.**

Managing access and security

The school will provide managed internet access to 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 regularly checked to ensure that it is working, effective and reasonable.

- The security of school IT systems will be reviewed regularly.

- The school will ensure that its networks have virus and anti-spam protection which are updated regularly by Eduthing.

- All staff and children will have their own usernames and passwords for services such as network user accounts, SIMS etc. Everyone will be made aware of the importance of keeping their login details confidential and not allowing others to access services using their log in details. Please see the Data Protection Policy that ensures we are GDPR compliant.

- Staff will be made aware of the importance of logging off and shutting down their computers at the end of the day. As well as protecting staff this ensures compliance with GDPR requirements.

- Supply teachers and student teachers have their own separate accounts to minimise opportunities for abuse.

- Children's use of the internet will be monitored by teachers in lessons and it is made clear to children that they are not allowed to delete internet history, which may be viewed by teachers at any time if necessary. Children are not allowed to use any device unsupervised by an adult.

- 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 school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

- Staff will receive regular training on the implications of the new General Data Protection Regulation which was introduced on 25 May 2018. The principles of this will be adhered to by all staff without exception.

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. All communication between staff and pupils or families will take place using school equipment and/or school accounts.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems. **Pupils will be advised not to give out personal details or information which may identify them or their location**

- Pupils must immediately inform the teacher if they receive offensive e-mails, or are aware that other children are sending or receiving offensive e-mails.

- Staff to pupil/parent email communication must only take place via a school email address or from within the learning platform.

- Incoming e-mail from unknown e-mail addresses should be treated as suspicious and attachments not opened unless the author is known. E-mails such as these should be transferred into the junk mail folder and reported to the Innovations Lead and Eduthing.

- **The school will consider how e-mail from pupils to external bodies is presented and controlled.**

Published content eg school website, school social media accounts

- The contact details will be the school address, emails and telephone number. Staff, governors' or pupils' personal information will not be published.

- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers, when children first join the school, before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/?a=168635.

- All material placed online by the school in any context is necessarily by consent. Staff, parents and children have the right to ask for any published material to be removed even if prior consent was given. Parents will be notified of this right on the consent form.

- A copy of all children who aren't allowed to have digital images taken and published on the school website will be available to all members of staff.

Use of social media including the school learning platform

- **The school has a separate social media policy.**

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.

- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.

- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school

community. Any slandering of the school through social media sites (including but not limited to Facebook, Instagram, Whatsapp, Skype, Snapchat, and Twitter) should be reported to the school immediately, appropriate action will then be taken.

- Pupils and staff will be advised never to give out personal details of any kind which may identify themselves or their location. They will also be taught about the importance of disabling location services when using mobile devices.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and is inappropriate for this age range.

- Pupils and parents will be advised that they have a responsibility to ensure that their own use of social network spaces outside school is respectful to all members of the school community and complies with the law.

- Parents will be advised at events such as school performances or special days such as sports days that any materials they have recorded must not be uploaded onto social media sites.

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the e-safety policy and the relevant AUP.

- Staff must not store images of pupils or pupil personal data on personal devices. Any non-compliance should be reported to the Data Manager for GDPR as a potential data protection breach.

- 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

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and, following its repeal, the General Data Protection Regulation 2018.

- The use of memory sticks is expressly forbidden in order to ensure that personal data is not lost should devices be lost or stolen.

- All devices which can in any way be used to access any personal information must be protected by a password or passcode. The loss of any school devices must be reported immediately so that hard drives can be remotely wiped by Eduthing.

- The use of personal devices for taking video or photos is limited to school trips and outings. All media must immediately be deleted from the device once it has been uploaded to the school system. (See Staff Code of Conduct Policy)

Policy Decisions
Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians) must read and sign the 'Staff Acceptable Use Policy' (AUP) before accessing the school IT systems.

- The school will maintain a current record of all staff and pupils who are granted access to school IT systems. The record will be kept up to date. eg. a member of staff may leave or a pupil's access be withdrawn.

- 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. However, reminders about what to do when discovering any inappropriate material will be given frequently.

- Children will not be allowed to use the internet at any time unsupervised by an adult staff member.

- People not employed by the school must read and sign the Acceptable Use Policy before being 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 audit computing provision and conduct child and parent surveys to establish if the Online Safety policy is adequate and that its implementation is effective.

- Youtube is currently not blocked for staff at Epsom Primary and Nursery School due to its huge potential in providing teaching and learning opportunities. However, the utmost care must be taken when using it. Videos must be checked before they are shown to children and teachers should be aware of dangers posed by autoplay and potentially inappropriate comments from other users.

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.

- Any complaint about staff misuse must be referred to the online safety team (of which the Headteacher will always be a part).

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of consequences and sanctions 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

To pupils

- Online Safety will be regularly and robustly taught to every child in the school, and material will be age-specific, focusing on the most critical aspects for that age group at that time.

- Online Safety rules will be visible in all classrooms and will be frequently discussed and revised.

- Pupils will be informed that network and internet use will be monitored, and that it is possible to track an individual's internet use.

- In addition to the age-related Online Safety advice, it will be made clear to pupils that the following activities are not permitted:

    I. Sending or displaying offensive or bullying messages or pictures.
    II. Damaging computers, computer systems or computer networks.
    III. Violating copyright laws.
    IV. Using others' passwords.
    V. Trespassing in others' folders, work or files.
    VI. Intentionally wasting limited resources.

- All Individual users of the internet are responsible for their behaviour and communications over the network.

- Computer storage areas and (any pupil use of) memory sticks will be treated like all school property. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or memory sticks will be private.

- Children will only be allowed to use the Internet when parental permission has been obtained.

To staff

- All staff will be shown where to access the e-safety policy and its importance explained.

- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet

- All staff will receive e-safety training on an annual basis

- Staff will be made aware of their responsibilities in ensuring that their own social-networking communications are professional, respectful and lawful.

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

- 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 will be offered e-safety training annually

- Parents, carers and anyone associated with pupils of our school community should ensure that their online activity takes into account the feelings of others in our community and is

appropriate for their situation as a member of the school community. Any slandering of the school or staff members through social media sites (including but not limited to Facebook, Instagram, Whatsapp, Skype, Snapchat, and Twitter) will not be tolerated. Any such items should be reported to the school immediately and appropriate action will then be taken.

Cyberbullying

NOTE: the term 'cyberbullying' is frequently used in the national media and so has been used in this policy to ensure clarity and understanding. However, many experts now believe the term is unhelpful as it necessarily implies a behaviour somehow distinct from bullying. Research shows that many children who wouldn't be happy to be called a 'bully' don't mind being thought of as a 'cyberbully'.

At Epsom Primary and Nursery School we will ensure that the term 'cyberbullying' is used alongside the term 'bullying'. A 'cyberbully' is a bully and that is important to emphasise.

- 'Cyberbullying' is the use of technology, particularly mobile phones and the internet, being deliberately used to upset someone else. Bullying is not new, but the following features highlight how cyberbullying is different from other forms.

i. 24/7 and the invasion of home/personal space
ii. The audience can be very large and reached rapidly
iii. People who cyberbully often attempt to remain anonymous
iv. Cyberbullying can take place both between peers and across generations

This is one of the reasons why it's important we all know how to respond!

v. Agree the rules for using technology
vi. Treat your password like a toothbrush – keep it to yourself
vii. Block the bully – learn how to block or report someone who is behaving badly
viii. Don't retaliate or reply!
ix. Always report cyberbullying – save the evidence – learn how to keep records of offending messages, pictures or online conversations
x. Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

Parents and Carers should:

- Use the tools on the service and turn on in-built internet safety features.

- Contact your child's class teacher if it involves another pupil, so that they can take appropriate action. When the school gets reports of inappropriate behaviour outside of the school, against a member of staff or another pupil, then the school behaviour policy will be followed. In extreme and unresolvable incidents the Headteacher may consider contacting the police.

Using the Internet safely at home

- As a family it is essential to have a common understanding of what is and what isn't appropriate behaviour online. It is also important to recognise the dangers posed by specific apps and websites.

Always:

i. Respect others
ii. Is careful about what they say and post online – including images

iii. Understands that anything posted can be made public very quickly and stays online forever. http://www.digizen.org/digicentral/family-agreement.aspx
iv. However, don't deny them the opportunity to learn from and enjoy the range of material and games that are available to them.

Simple rules for keeping your child safe

➢ Keep your computer secure

Run a firewall, anti-virus, and content filtering software, and keep them up to date
Keep computers in a family area – don't' forget the internet can be accessed through a whole range of devices: desktops, laptops, tablets, phones, e-readers and online gaming.
Children should use a strong password – phrases such as 'dogatehomework' are better than short words such as 'dog'- and share with an adult.

➢ Know what your child is doing in the Internet

This doesn't necessarily mean needing to accompany them at all times, especially with older children. However, some monitoring may be required especially if they are playing games that allow users to contact each other through online messaging (voice or on-screen).

➢ Your child should ask permission before using the Internet – this includes any games that have a social networking element.

➢ They should only use websites, games and search engines that you have chosen together.

➢ Only chat or email with people that you know – maybe you could set up an address book.

➢ Have a look round the site or game, so that you can assess it for yourself.

Keep personal information private

- Never use a real name – create a nickname.
- Never give out personal information such as address, phone number, name of school, pictures in school uniform.
- Many sites require registration, and most trustworthy sites require adults to register and explicitly allow their child to participate.
- Be aware of the information that you share when sharing images online e.g a first day at primary school photograph could give details of your child's school, where you live, car number plate etc.
- Ensure children know never to arrange to meet someone they have 'met' on the Internet without talking to an adult first; if they do meet always take an adult and meet in a public place.
- Ensure children know only to use a webcam with people they know and that webcams should be covered when not in use as they can be taken over by criminals.

➢ Ensure they tell you immediately if they see anything they are unhappy with

- Ensure that you know where to go to get more help - e.g. Contacting staff at Epsom Primary and Nursery School or reporting the incident at https://www.ceop.police.uk/safety-centre/.