SPRINGFIELD SCHOOL

E-Safety Policy

Approved: May 2023 Review date: May 2024

Pupils interact with new technologies such as smart devices and the internet on a daily basis. These are viewed as essential elements in 21st century life for education, business and personal communication. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place users in danger, so not only does the school have a duty to provide students with quality, filtered internet access as part of their learning experience but also a 'duty of care' to keep pupils safe by raising awareness of the risks involved and highlighting the responsibilities that accompany sensible use. We are particularly mindful of our responsibilities to raise pupils' awareness of 'grooming' techniques used on the internet as well as preventing access to terrorist and extremist material when accessing the internet in school and promoting resilience to radicalisation.

A significant amount of the material on the internet is published for an adult audience and much is unsuitable for young people. Springfield School aims to achieve the right balance between controlling access, setting rules and educating students for responsible use. We will work with parents, our pupils and other members of our community to develop complementary strategies to ensure safe, critical and responsible ICT use at all times, both in and out of school.

This policy forms part of the 'e-safety package' - a comprehensive set of documents and actions which relate to the safe use of the internet, mobile 'phones and other electronic communication technologies by members of the Springfield community. In following the principles below staff will also observe the guidance laid out in the DfE publication 'Teaching Online Safety in Schools' (January 2023 update) which is linked below.
https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

- Instruction in responsible and safe use will precede and accompany internet access at Springfield. All Springfield staff are responsible for promoting e-safety both in school and at home. Specific instruction is delivered through the ICT programmes, assemblies and the PDL curriculum.
- Pupils are taught how to evaluate internet content, to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are required to re-affirm their understanding and acceptance of the induction document message at the beginning of each academic year.
- Staff are required to review the 'Responsible use of ICT: Staff' document in the Staff Handbook on an annual basis, each September and re-affirm their commitment to following agreed protocols as well as acceptance of the conditions attached to their personal use of ICT hardware/software.
- Members of the community using our facilities will also be required to sign an 'Acceptable use statement'.
- E-safety posters will be on display in all networked areas.
- E-safety information and guidance for pupils and parents will be updated and shared via the school's website and, where possible, during events such as parent's information evenings.

The E-Safety policy is intended to enhance values laid out in the Equality Policy. In particular, by:

- Ensuring that respect for others is considered in all electronic communication and publications.
- Providing a safe learning environment whilst allowing access to as full a range of technologies and social developments as possible.
- Protecting members of the school from any kind of harassment or discrimination using new technologies.
- Ensuring, through policy and practice, that the school has systems in place to effectively challenge, combat and repair discriminatory behaviour towards members of the school community caused by any infringement of this policy or the ICT acceptable usage policies.

GENERAL GUIDELINES:

The school internet access is provided by Portsmouth City Council (PCC) and includes primary filtering appropriate to our school and the age of pupils. The school leadership team/ICT Network Manager control secondary internet filtering and have responsibility to ensure access and restriction settings are appropriate for staff and students. All reasonable precautions are taken to ensure that filtering is age appropriate and set to prevent access to all inappropriate material whilst maintaining all the educational benefits of internet access. 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 PCC can accept liability for the material accessed, or any consequences of internet access. If staff, pupils or community users inadvertently discover an unsuitable site, it should be reported to the Network Manager who will liaise with the Designated Safeguarding Lead (DSL) to get it blocked. Where staff make requests for suitable (new) sites to be unblocked, this will be reviewed by the DSL/Network Manager. The school works to ensure that systems to protect users are reviewed and improved in line with any new developments.

Please see Appendix 1: (Flowchart of internet filtering)

- Virus protection will be installed and updated regularly.
- Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.
- Network and internet use is subject to monitoring.
- Copying and subsequent use of internet derived materials by staff and pupils must comply with copyright law.
- All users are responsible for the security of their own passwords and activity when their password has been used to logon. Computers should not therefore be left unattended when an individual is logged in or passwords shared with other individuals.
- The school will maintain a current record of all staff, pupils and community users who are granted access to school ICT systems. All users should ensure that their use is legal and ethical as well as reflecting the standards of the school community. The school reserves the right to withdraw access to any user who does not demonstrate responsible use.
- The use of school computer equipment and systems, including internet use, is monitored by network staff. Any misuse will be reported by network staff or supervising teachers on SIMS Behaviour module and categorised as appropriate and referred to the appropriate Year office for sanctions to be applied. Complaints of internet misuse involving cyber-bullying will also be dealt with by the Heads of Achievement but also reported to the designated member of staff for inclusion in ClassCharts behaviour records. Any complaint of staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures and referred immediately to the school's Designated Safeguarding Lead.
- All members of the community can report concerns over specific internet sites to the Child Exploitation and Online Protection Centre (CEOP) using the link: http://ceop.police.uk

- Concerns regarding potentially 'extreme' online behaviours will be reported to the Police and the Multi-Agency Safeguarding Hub (MASH) via an inter-agency referral form

E-MAIL AND MESSAGING (including messages/comments within Google Classroom):

- All staff and pupils (where educational purposes require it) are provided with a school email address or local messaging system. Users must be aware that communication may be monitored.
- Staff should not be in personal email contact with existing school pupils. Ring fenced school communication methods must be used.
- Access in school to external personal e-mail accounts may be blocked.
- Pupils must immediately tell a teacher if they receive offensive or worrying e-mails or messages. Staff must report any offensive or inappropriate e-mails or messages received to their link member of SLT.
- Attachments must not be opened unless they are expected and from a known sender.
- Pupils must not reveal personal details or images of themselves or others in electronic communications.
- All electronic communications sent to external organisations should be written carefully, in the same way as a letter written on school headed paper. Internal communications should be treated with similar care and respect.
- Staff should aim to send (or time) messages within 'working hours' only i.e. 8am-6pm on working days.

SOCIAL NETWORKING AND PERSONAL PUBLISHING:

- The school will normally block/filter access to social networking and artificial intelligence (AI)/'chatbot' sites (other than those within the VLE) unless short-term access is required for a specific educational project.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not share explicit images on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.
- Staff should not have a CURRENT pupil or ex-pupil under eighteen years of age as a contact on any social networking site (N.B. for children/adults deemed 'vulnerable' staff must refrain from any contact of this type regardless of age).
- Staff should be mindful of the current guidelines on professional conduct at all times when interacting with colleagues/friends on networking sites.
- No comments should be posted on social networking sites, websites or via email that could cause offence or impact on the reputation of the school or individuals within it. All comments posted on social networking sites should be considered to be public. Privacy settings should not be relied on for privacy.

PUBLISHED CONTENT ON THE SCHOOL WEB SITE:

- Contact details and web content are restricted and monitored by a member of SLT.
- Photographs of pupils involved in school activities or examples of their work may be included on the school's website as stated in the Home-School Agreement and where consent is given. If parents/carers wish to withdraw permission then they should put their objections, in writing, to the Headteacher.

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.
- Bringing a phone into school is entirely at an individual's own risk and the school is not liable for any damage/loss/theft/misuse.
- The sending or posting of abusive, offensive or inappropriate messages by any member of the Springfield community is unacceptable and will lead to sanctions being applied. External authorities may be notified where it is felt to be justified.
- Taking or using digital images without prior permission is prohibited.
- Staff must use a school telephone where direct verbal contact with pupils is required.

Mobile Phones and Electronic Devices

- Pupils are permitted to have mobile 'phones and/or electronic devices (e.g. smart watches) with them in school although there is no curriculum requirement for pupils to do so. If brought into school they should be switched off completely and out of view at all times. Pupils must not use their 'phones or devices anywhere on the school site before or after school, nor during break and lunchtime so as not to compromise the safety of other pupils in accordance with the mobile phone/device guidelines.
- Any pupil found to be using a mobile phone/device (or when a mobile phone/device 'sounds' in anyway) will have the phone/device confiscated by the member of staff; the student will be issued with a standard letter and arrangements made for the phone or device to be collected at a convenient time by parents/carers
- The school does not accept liability for items brought onto the school which become damaged, lost or stolen and would encourage students not to bring expensive items onto the school site.

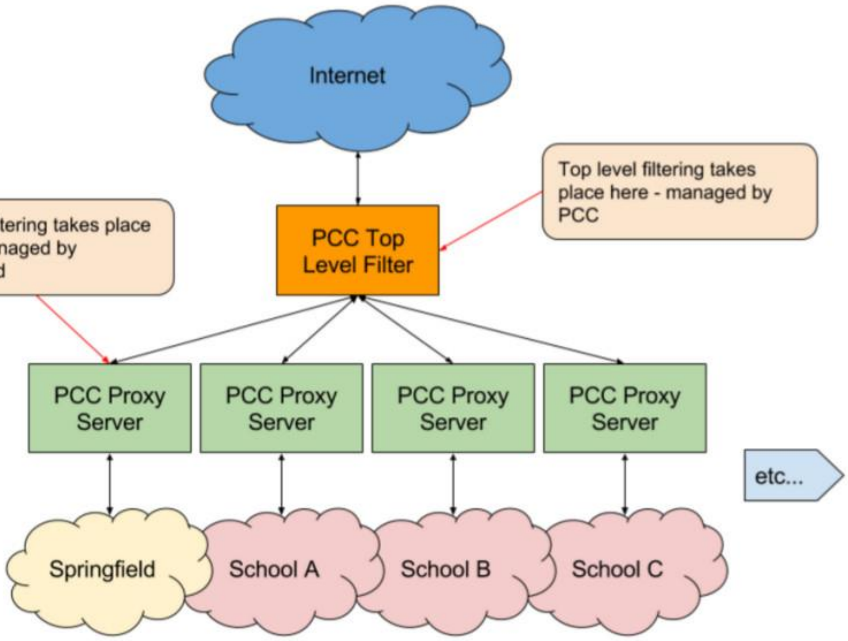
Equality Policy Compliant

This policy should be read in conjunction with the following Springfield policies/procedures:

Safeguarding and Child Protection
Data Protection
Disciplinary
Remote Education Provision: Information For Parents
Acceptable usage of ICT/Electronic Media Policy
DCT Code of Conduct (Staff)
Teachers' Professional Standards

APPENDIX 1

Appendix 1: Filtering Flowchart


Internet
Top level filtering takes place here - managed by PCC
PCC Top Level Filter
Internet filtering takes place here - managed by Springfield
PCC Proxy Server
PCC Proxy Server
PCC Proxy Server
PCC Proxy Server
etc...
Springfield
School A
School B
School C