E-SAFETY POLICY

This policy covers all pupils from age 3 – 19 years across the Junior and Senior School including the Early Years Foundation Stage (EYFS) and anyone who works within the school community.

DEFINITION OF E-SAFETY FOR PURPOSES OF THIS POLICY:

E-Safety encompasses use of the Internet and all electronic communications via computers, mobile phones, tablets, handheld devices, games consoles and wireless technology both on and off the school site where associated with school or where usage impacts on the school community. It includes, but is not restricted to the following:

- Safe online behaviour
    - Behaving with respect for others and protecting own online reputation
    - Have an understanding of what constitutes cyberbullying, sexting, grooming, abuse and radicalisation
- Using social networking sites safely and responsibly
    - Ensuring any posts and comments are appropriate and do not bring the name of the School into disrepute; abiding by any age restrictions for holding an account
- Responsible electronic communications
    - Via text message, email, mobile phone apps, social media posts and blogs etc.
- Protection of personal details
    - Ensuring that name, age, address, bank details etc. are never shared online
- Exercising judgement when using the Internet
    - Accessing appropriate content on the Internet, knowing how to report anything inappropriate and/or suspicious both inside and outside of school
    - Checking the validity and reliability of information found online.
- Email safety
    - Awareness of how to deal with ‘spam’ and ‘phishing’ emails, only trusting ‘known’ senders, particularly when opening attachments.
- Security awareness
    - Creating strong passwords, keeping passwords private, being aware of viruses and hacking

- Respecting copyright and intellectual property laws when sharing or downloading files

- Knowing how to report an issue both within and outside school

    - Talking to a responsible adult about any issues, taking a 'screenshot' as evidence, using 'Click CEOP' if needed

STATEMENT:

The Royal Russell School E-Safety Policy is designed to protect pupils, all staff who work at the School and protect the School itself with particular reference to those the risks that are posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.

The School recognises that use of the Internet and electronic communications are an increasingly important part of everyday life for all within the school community. This technology can be used to enhance teaching, learning and communication (examples could include emailing work between pupils and teachers, using the Internet for research, sharing a photo/recording of a performance and use of virtual learning environments such as Firefly to create and share lesson resources with pupils). The School has clear protocols on the reporting of misuse of the Internet and electronic communications and the support available to those who are the subject of bullying, grooming, abuse or radicalisation.

An effective learning platform or virtual learning environment (VLE) offers the school a wide range of benefits to teachers, pupils and parents, as well as support for management and administration. It can enable pupils and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and pupils can develop online and secure e-portfolios to showcase examples of work.

- Pupils/staff will be advised about acceptable conduct and use when using the VLE
- Only members of the current pupil, parent/carers and staff community will have access to the VLE.
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff, pupils etc. leave the school, their account or rights to specific school areas will be disabled**.**

AIMS:

The School is committed to ensuring pupils are using the Internet and electronic communications in a safe and responsible way. The School expects and promotes good conduct, behaviour and etiquette online both inside and outside of school.

E-Safety education is delivered across the Junior and Senior School curriculums through:

- Lessons in E-safety education in the Computing and PSHE curriculum, including visiting speakers
- Form/House/tutorial sessions
- School Assemblies, House Assemblies and Chapel
- Parent Awareness Evenings
- School broadcast communications; for example, the Headmaster's Newsletter or Junior School Bulletin
- Staff induction sessions, INSET and training.
- Digital Leaders initiatives

The misuse of Information and Communication Technologies, including but not limited to the activities above, will result in disciplinary sanctions in line with the Staff Disciplinary Procedure (staff) / School Behaviour Policies (pupils). Any evidence of inappropriate and/or illegal behaviour will be dealt with in the **strongest possible** terms.

Staff will be vigilant in monitoring misuse of technology and will be readily available to listen to pupils who feel they have concerns regarding E-Safety.

Internet access through the school system is strictly filtered and monitored 24/7 and any breaches of this system are reported by the Network Manager to an E-Safety Coordinator or a member of SLT.

Pupils and parents should be aware that most social media sites have regulatory age limits. Most sites require members to be over the age of 13. Terms and conditions should be read carefully prior to signing up for an account. The school wired network blocks all social media access during the school day for pupil access (exemptions are via department and permission from a member of SLT).

DEALING WITH INCIDENTS (pupils):

- The incident will be investigated by the member of staff making the discovery and details will be recorded on My Concern.
- This form will be passed to the E-Safety Coordinators, heads of house, or DSL as appropriate.
- Should the incident involve inappropriate images, the DSL should be contacted as soon as possible. The E-Safety Coordinators conduct further investigation and will escalate the matter to a member of SMT if required
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- The IT support team may be required to provide technical input as part of the investigation.
- Parents/guardians will be kept informed by the school in line with the School Behaviour Policies.
- Sanctions will be determined in line with the School Behaviour Policies.
- If there is a concern that a young person is harmed or at risk of harm, a referral should be made to children's social care and/or the police in line with the Safeguarding Policy.

DEALING WITH INCIDENTS (staff):

- The incident should be reported to the line manager of the member of staff involved and details will be recorded on My Concern.
- The Line Manager will conduct further investigation and will escalate the matter to a member of SLT if required.
- The IT support team may be required to provide technical input as part of the investigation.
- The member of staff involved will be kept informed by the school in line with the Staff Disciplinary Procedure.
- Sanctions will be determined in line with the Staff Disciplinary Procedure.

Radicalisation and Extremism:

As part of the Prevent agenda, the School will ensure an effective filtering and monitoring system to prevent radicalisation and access to extremist views.

Staff will be made aware at safeguarding training of the characteristics within children and families that may indicate radicalisation or warning indicators of those who may be vulnerable to radicalisation. The school's Safeguarding Policy, which is available on our website (www.royalrussell.co.uk) and in school, covers Radicalisation and Extremism (see pages 58 and 59 of the Safeguarding Policy).

Reporting concerns regarding radicalisation and extremism:

Staff will treat any radicalisation/extremism concerns in the same manner as safeguarding concerns and will follow the school's child protection and safeguarding procedures.

As part of the ICT AUP agreement, pupils agree not to seek extremist material.

The School will not tolerate behaviours such as:

- Any form of bullying or cyberbullying
- Sexting
- Any online behaviour accessing extremist content
- Sending or accessing inappropriate content, including websites
- Posting inappropriate comments/photos on social media, blogs etc.
- Taking, uploading or sharing photos, videos or audio recordings without permission
- Unauthorised use of devices, as referred to in the Mobile Electronic Devices Policy
- Any activity which may bring the school's name into disrepute
- Infringement and disregard for Copyright Law and or intellectual property rights
- Identity theft, including sharing passwords and unauthorised access to school and personal accounts held online, for example Gmail, Facebook, Twitter and Instagram.

SEARCHES:

STAFF AUTHORISED TO CARRY OUT SEARCHES, DELETION OF DATA OR FILES:

If an authorised member of staff has reasonable grounds for suspecting that a pupil / staff member is in possession of data that is inappropriate or against the terms of use, s/he is entitled to conduct a search. The authorised member of staff should take care that, where possible, searches should not take place in public places such as an occupied classroom, which might be considered as exploiting the pupil / staff member being searched; there must be a witness (also a staff member) and, if possible, they too should be the same gender as the pupil / staff member being searched.

In some cases, if s/he has reasonable belief that there is a risk that serious harm will be caused to a person if the search is not conducted immediately, s/he may conduct this search in the absence of a witness, but only where it is reasonably believed that there is a risk that the serious harm will be caused to a person if the search is not conducted immediately, and where it is not reasonably practicable to summon another member of staff. Care should be taken not to delete material that might be required in a potential criminal investigation.

Those authorised to conduct a search are as listed below:

- The Headmasters
- The Deputy Heads
- The E-Safety Coordinators
- IT Systems and Network Manager
- The Head of Sixth Form
- Housemasters/mistresses.

The person conducting the search may search any devices or accounts that the pupil / staff member appears to have control over. Desks, lockers and bags can also be searched.

For safeguarding, security, compliance and maintenance purposes, the School reserves the right to examine and/or delete any files that may be held on its systems. Authorised users will monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or us-

ers on the Royal Russell School network may be disconnected. Information Security prohibits actively blocking authorised audit scans. The Schools Firewalls and other blocking technologies permit access to the scan sources.

SPECIFIC AREAS OF RESPONSIBILITY:

Governing Body: The Chair of Governors will ensure that the School has a policy and this is known to all members of teaching staff.

Headmasters: The Headmasters have an obligation to draw up procedures to prevent E-Safety incidents occurring amongst pupils and pupils**.**

The Headmaster and the Headmaster of the Junior School will:

- Ensure that all staff have an opportunity to discuss strategies and review them
- Determine the strategies and procedures
- Discuss development of the strategies with the School Leadership Team
- Ensure appropriate training is available
- Ensure that the procedures are brought to the attention of all staff, pupils and parents/guardians

Designated Safeguarding Lead (DSL):

Should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- radicalisation and exposure to extremist material

E-Safety Coordinators

The E-Safety Coordinators will:

- Be responsible for the day-to-day management of the policy and procedures
- Ensure that there are positive strategies and procedures in place to help both the victims and perpetrators
- Keep the Senior School Housemaster/mistress and Junior School Class Teacher informed of all incidents
- Arrange relevant staff training
- Determine how best to involve parents/guardians in the solution of individual problems
- Make an annual report to the Headmasters.

All Staff will:

- Know and implement the current policies and procedures
- Report all incidences regarding E-Safety, whether on-site or during an off-site activity.

Pupils, staff and families, when on site will:

- Use the Internet in support of academic work or personal interests which are consistent with the values of Royal Russell School and its Code of Conduct.
- Ensure any music, films and files are downloaded legally (i.e. not through unauthorised file-sharing sites), and do not breach copyright laws.
- Use the school's 'safe' internet connection and will not attempt to bypass this service with the use of VPNs or other methods. Pupils attempting to access proxy sites, torrent sites or adult material may have their Internet privileges restricted.

MONITORING AND EVALUATION:

- A '360 Degree Safe' working group consisting of the Safeguarding governor, the DSL, E-Safety Co-ordinators, the IT Manager and parent and staff ambassadors meets regularly to produce and review E-Safety policies, review and adapt the E-Safety Curriculum, review and monitor the school filtering policy and raise awareness of E-Safety throughout the community. This group will collate reports on serious incidents and prepare an annual report for the Headmasters.
- The Headmasters will consider the reports, with the School Leadership Team, to determine what can be learned from the incidents and how they were handled with a view to improving the School's strategies
- The Headmasters will update the Governing Body as part of the Safeguarding report on an annual basis.

ORIGIN OF THE POLICY:

This policy has been created by the E-Safety coordinators in consultation with the School Leadership Team.

LINKS:

This policy links with:

- Anti-Bullying Policy
- Behaviour Policies
- Safeguarding Policy
- Staff Disciplinary Procedure
- Whistleblowing policy
- ICT Acceptable Use Policy
- Prevent Policy
- Mobile Electronic Devices policy

WEBSITES:

https://www.ceop.police.uk/safety-centre
www.thinkuknow.co.uk
www.saferinternet.org.uk
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf
www.childnet.com/
www.rm.com/_RMVirtual/Media/Downloads/E-Safety-Guide-A5v6-proof.pdf
https://www.gov.uk/government/publications/channel-guidance

Reviewed	September 2018
Reviewed by	SLT and E-Safety Coordinators
Reviewed and Approved by EWC	October 2018
Reviewed and Approved by Board	December 2018
Reviewed by	SLT and E-Safety Coordinators
Reviewed and Approved by EWC	February 2020
Reviewed and Approved by Board	March 2020
Next Review	January 2022