ONLINE SAFETY POLICY

This policy covers all day and boarding 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.

This Policy should be read in conjunction with:

- Keeping children safe in education 2025
- Meeting digital and technology standards in schools and colleges (2022)

At Royal Russell (hereafter referred to as 'the school') we recognise that pupils will have access to technologies that have both positive and negative potential. The school also recognises the enormous benefits - to pupils and staff - of the internet as a means of academic research, for entertainment and for social interaction, and seeks to promote and encourage its effective use. The school is fully aware that online safety is directly related to safeguarding and takes seriously its responsibility to advise students, parents and staff of the significant dangers digital technologies can present when used inappropriately, whether this misuse be deliberate or unwitting. This policy applies to all members of the school community (including staff, pupils, resident families, parents, visitors) who have access to and are users of school ICT systems, both in and out of the school and should be read in conjunction with the relevant Acceptable Use Policies (AUPs), which offer clear guidance on the use of technology in the classroom and beyond for all users.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

• **content:** being exposed to illegal, inappropriate or harmful material, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation extremism, misinformation, disinformation (including fake news) and conspiracy theories.

• **contact:** being subjected to harmful online interaction with other users, for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. Concerns about this type of risk to pupils, students or staff, should be reported to the Anti-Phishing Working Group: APWG | REPORT PHISHING.

The safe use of ICT is an issue of behaviour, education, infrastructure and monitoring; it is fundamental to safeguarding pupils and staff both in and out of School.

The school takes all reasonable precautions to ensure that users access only age-appropriate material, that content accessed via school devices and systems is appropriately filtered and monitored, and to educate pupils about online dangers. However, experience shows that it is not possible to guard against every danger and so we take a proactive approach to minimising risks whilst also

educating pupils so that they can respond appropriately to an unsafe situation. Risks are considerably greater where devices are beyond the school's control (4G, 5G, social media platforms etc.) and so the education aspect of online safety is ~~safeguarding in this area is~~ particularly important. Getting pupils into safe habits when accessing the online world via our systems should enable them to make the right choices when using their own connections. A key part of the online safety support in the Junior School is to share this information with parents. In the Senior School pupils are taught about privacy settings for their devices and accounts.

Ensuring boarding pupils are safe online and not accessing or exposed to inappropriate material is essential. While our filtering and monitoring provision (see below) has a significant role to play here, this alone does not prevent the possibility of boarders using the mobile networks listed above to access inappropriate content, nor from their bringing inappropriate content to school already downloaded onto a device. In caring for our boarders, the School seeks to balance our duty of care to keep them safe with their rights to privacy and a homely environment. We adopt a profiled approach to mobile devices, which sees pupils up to Year 9 inclusive hand their devices in at bedtime, while our Y10, 11, 12 and 13 are trusted to hold theirs and behave responsibly. However, any online safety concerns about individual pupils in these older years will lead to investigation and support and/or sanctions to manage this behaviour, including the temporary (eg overnight) or routine (eg every night) confiscation of a device. We encourage pupils to report concerns that they have about inappropriate content on a device or about undisclosed or secret devices, supporting this with assemblies and Wellbeing lessons which highlight the importance of making responsible choices online.

It is important to be aware that safeguarding concerns can happen solely offline or solely online, but that it is often the case that issues can happen concurrently both in the real world and online. Whenever considering any offline issue the staff involved should always explore whether there is also any online component.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, visitors, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Definition and scope:

Online safety encompasses use of the Internet and all electronic communications via computers, mobile phones, smart watches, tablets, handheld devices, games consoles and wireless technology both on and off the school site if associated with school or if 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 one's own online reputation
    - Having an understanding of what constitutes cyberbullying, nudes and semi-nudes, grooming, abuse ~~and~~ radicalisation misinformation, disinformation (including fake news) and conspiracy theories.
    - Understand the risks associated with the use of AI tools, including that they can produce content that is inaccurate, biased, or inappropriate for young users, the dangers of sharing of personal information including photos, and the possibility of emotional attachment or overreliance on chatbots.

- **Using social networking sites safely and responsibly**
    - Ensuring any posts and comments are appropriate and do not bring individuals or the name of the school into disrepute; abiding by any age restrictions for holding an account
- **Responsible electronic communications**
    - Via text message, email, group chats and other social networking apps, social media posts and blogs etc.
- **Protection of personal details**
    - Ensuring that name, age, address, bank details and other personal details etc. are never shared online or with AI systems.
- **Exercising judgement when using the Internet**
    - Accessing only 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 and that produced by AI tools.
- **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 CEOP's 'Make a Report' if needed

3. Oversight of online safety

a. Online Safety Committee

The DSL meets with the 'online safety committee' at least once each term to review relevant school processes and discuss any incidents or patterns. This committee consists of The DSL, The Senior Deputy Head, Deputy Head (Pastoral) and DSL of the Junior School, and the Assistant Head (Innovation and Digital Learning). The Network Manager and the DSL are responsible for evaluating our filtering and monitoring provision and for procuring systems required to support this area.

The online safety committee and its members take responsibility for monitoring the overall effectiveness of our systems and procedures, identifying any education needs that arise and implementing changes in these systems and procedures as necessary.

b. Reporting Concerns (including Safeguarding concerns)

Online safety is a whole school responsibility and pupils, parents and staff should report any issues or concerns in relation to online activity or digital technology to any member of the Online Safety Committee.

If the matter relates to safeguarding, it should be reported to the Designated Safeguarding Lead in the Senior or Junior School or one of the Deputy Designated Safeguarding Leads. If none are available, the matter should be reported to a member of the school's senior leadership team.

If a member of staff believes a child is suffering or likely to suffer from harm, or is in immediate danger, they must contact children's social care and/or the police immediately. Anyone can make a referral of this sort, but the DSLs (or deputies) can support with this and will usually take responsibility for taking this action. Information about how to make a referral can be found in the Safeguarding and Child Protection Policy.

A particular risk faced by young people online is that they may be radicalised or drawn into extremism. All members of staff receive safeguarding training on the Prevent Duty as part of their routine updates, at least annually, in order that they are able to recognise warning signs in relation to a pupil's online or offline behaviour in relation to this risk.

~~Anyone who teaches, coaches or supervises Royal Russell pupils can make a direct referral to external safeguarding authorities at any time should they feel concerned about the welfare of a pupil.~~

~~For concerns about the behaviour of an adult who works with children, the contact details for the Local Authority Designated Officer are:~~
~~Local Authority Designated Officer (LADO):~~
~~Senior LADO: Steven Hall~~
~~LADO: Jane Parr~~
~~Business Support Officer: Karen Anns~~
~~Direct line: 020 8255 2889~~
~~lado@croydon.gov.uk~~

~~For concerns about a child, in Croydon, child protection referrals should be made to the 'Multi-Agency Safeguarding Hub' (MASH) and 'Early Help' Professionals' consultation line~~
~~Tel: 0208 726 6464~~
~~Out of Hours Tel: 0208 726 6400~~

~~Referrals for students living outside the borough of Croydon will be made directly to the safeguarding team of the appropriate local authority. Reports of concerns under the Prevent duty should be made to: safercroydon@croydon.gov.uk~~

~~Further details about making referrals can be found in the Safeguarding and Child Protection policy.~~

c. Filtering and Monitoring

As per KCSIE 2025, the appropriateness of filtering and monitoring systems is a matter for the school and is informed in part by the Prevent Duty. At Royal Russell, online activity is proactively filtered and monitored using commercial products. These products block staff and pupil access to inappropriate sites (e.g. gambling and pornography) and provide reports of any attempts by pupils and/or staff to access inappropriate sites. The list of sites blocked by these filters are routinely updated by the service providers.

As per the Department for Education filtering and monitoring standards, the school:

- Identifies and assigns roles and responsibilities to manage filtering and monitoring systems

- Reviews filtering and monitoring provision at least annually
- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning
- Has effective monitoring strategies in place to meet safeguarding needs

The governing body will review these standards and discuss with the DSL in the Junior and Senior School and with IT staff ~~and service providers~~ what more needs to be done to support the school to meet this standard

The school's filtering and monitoring system works on all school-issued devices whether they are on site or away from school. Whilst the filtering system works 24 hours a day, monitoring requires human intervention and so for day pupils this is only in place term time during working hours and we inform parents of this. Personal devices are not subject to Filtering and Monitoring, unless accessing school Wi-Fi onsite; Pupils below the Sixth Form are not allowed access to personal devices during the school day, which ensures that they cannot access unfiltered content.

To manage the risks presented by the use of AI tools, the schools filtering and monitoring system diverts pupils using school devices into securly's safe AI chat.

To meet the specific needs of Boarding pupils who live onsite and must have access to systems that allow contact with family members in their home country, a less restrictive policy is in place after school hours on weekdays and across the weekend. ~~a 'Boarding Wi-Fi' is available, this is only available within the Boarding Houses.~~ This is subject to filtering and monitoring, but allows access to VPNs for communication with family members. The filtering and monitoring system has a policy applied so that the devices attached to the policy are not able to access the internet between 12am and 6am overnight to ensure that pupils do not have unsupervised access to the internet and potentially harmful content and that they do not suffer from disrupted sleep from using devices. Younger pupils (Y7-9) must hand in all devices except school devices at bedtime.

Boarders devices are monitored overnight and at weekends during term time, by the Securly On-Call product. Contact is made with school staff during these out-of-hours times if there is any self-harm or suicide related flags. Other alerts that happen during weekend or night times are addressed during the next school day.

Breaches are reported using a categorisation system which is automated but also monitored and managed by the IT Manager. Breaches are then investigated as required by the appropriate member of staff; the decision on who does this will be taken by the DSL of the relevant school (Senior or Junior).

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).

d. Virtual Learning Environment (VLE)

The school's VLE is an important aspect of our approach to online safety:

- Pupils and parents have access to Online Safety Advice via the Safeguarding pages
- Pupils can report cyberbullying (and offline bullying) to school via the 'report bullying' button
- There is a link to Childline's 'Report Remove' service through which they can access expert help to remove nude images posted online

- There is a link to CEOP (Child Exploitation and Online Protection - a National Crime Agency command) through which they can report safeguarding concerns about online abuse or grooming.
- ~~Pupils/staff will be advised about acceptable conduct and use when using the VLE~~
- ~~All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.~~

The VLE is a secure area, only available to the Royal Russell community.

- Only members of the current pupil, parent/carers and staff community will have access to the VLE.
- When staff, pupils etc. leave the school, their account or rights to specific school areas will be disabled**.**

4 . Online safety education

a. Pupils

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.

Online safety education is delivered across the Junior and Senior School curricula through:

- Lessons in online safety ~~e-safety~~ education in the computing ,Wellbeing (Senior School) and PSHE (Junior School) curricula, including visiting speakers
- Form/House/tutorial sessions
- School assemblies, house assemblies, year group assemblies and chapel services (where appropriate)
- Parent awareness evenings
- School ~~broadcast~~ communications; for example, the Headmaster's Newsletter or Junior School Newsletter and Friday emails
- Staff induction sessions, INSET and training.
- Junior School Digital Ambassadors' initiatives
- ~~Digital leaders' initiatives~~

Our approach to education of pupils in online safety:

- Encourages pupils ~~to work with us and~~ tell us when they have concerns.
- ~~Tries to maintain good channels of communication rather than 'over-blocking' sites, so that pupils let us know when they get into difficulties.~~
- Takes pupils through the Acceptable Use of ICT Policy every year in a Computing (JS) or Computer Science (SS) lesson, year group assembly asking pupils to sign the agreement online.
- Educates pupils via the Wellbeing curriculum (Senior School) and PSHE (Junior School) curriculum about how to stay safe online and how to report concerns, as well as through the assembly programme if/when additional updates are needed.
- ~~Gives other reminders in House meeting as well as in Assembly about online behaviour~~
- ~~Has Wellbeing lessons, and chapel service focusing on how to stay safe, as well as legal updates.~~
- ~~Informs pupils when changes happen to keep them safe.~~
- ~~Uses Wellbeing programme, Computer Science lessons and the Pupil Induction Programme to promote safe behaviour online.~~
- ~~Asks Senior Prefects to promote safe behaviour online and to work with pupils to ensure their privacy settings are up to date and appropriate.~~
- Keeps parents informed through workshops and newsletters.

- Reminds pupils regularly (though Wellbeing / PSHE curriculum and other opportunities such as House / Year or Whole School assemblies) ~~annually~~ about the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to anyone.
- ~~Has a group of senior pupils, the 'Digital Leaders', who regularly visit House and talk to pupils about online safety issues.~~

b. Staff

It is essential that staff granted access to the school's IT networks receive education and training. This is achieved through the following means:

- Staff induction for new joiners
- Ongoing annual updates plus additional information provided as and when appropriate (for example, when legislation changes or there is a new platform or device to use, or when there is an Online Safety update that needs to be shared sooner)
- Confirmation that staff have read and understand the relevant policies, including:
    - Staff acceptable use policy
    - Staff Code of Conduct
    - KCSIE updates
    - Online Safety Policy
    - Safeguarding and Child Protection Policy
- The school subscribes to a commercial provider of ongoing training overseen by the network manager, currently consisting of Censornet courses sent to all staff.
- ~~**Radicalisation and Extremism (Prevent Duty):** 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 covers Radicalisation and Extremism.~~

c. Parents

Parents play an essential role in the education of their children and in the monitoring/ regulation of the children's on-line behaviours and interactions with digital technologies. The school will provide information about online safety to parents through newsletters and parent information evenings ~~and seminars.~~

d. Governors

Oversight of the School's Online Safety provision is via the work of the Education and Welfare Sub-committee.
The Online Safety governor is the Chair of the Education and Welfare Sub-Committee, and he meets with the DSL termly to discuss safeguarding matters including online safety. ~~is provided with opportunities to attend safety training sessions provided by professional organisations.~~

5. Dealing with online safety related incidents:

a. Pupils

The School takes ~~will adopt~~ a **zero tolerance approach** to any cyber bullying issues. Staff or pupils who become aware of a cyberbullying incident should report this to the relevant Housemaster / Housemistress in the Senior School or the Pastoral Deputy Head and DSL in the Junior School.

Safeguarding concerns related to online behaviour of pupils must be reported immediately to the DSL if they relate to pupil behaviour and to the Headmaster if they relate to staff behaviour. These concerns will be managed in line with the school's Behaviour Policy (pupils) and Staff Code of Conduct (staff).

See **Appendix 1** for **guidance on what to do in the event of discovering content containing indecent images of children or criminally obscene adult content**

The school will not tolerate behaviours such as:

- Any form of bullying or cyberbullying
- Sharing of nudes or semi-nudes, including those produced with the aid of Generative AI tools.
- ~~Any online behaviour accessing extremist content~~
- Sending or accessing inappropriate online content, including extremist content. ~~, including websites~~
- Posting inappropriate comments/photos on group chats, social media platforms, blogs etc even when this content is encrypted or in a closed group.
- Taking, uploading or sharing photos, videos or audio recordings without permission
- Unauthorised use of devices, as referred to in the Behaviour Policy. ~~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, including email accounts, social media accounts, direct messaging services and group chats.~~, for example Gmail, Facebook, X (Twitter) and Instagram.~~

These will be dealt with according to the Behaviour Policy, the Anti-bullying Policy and the Safeguarding and Child Protection Policy as appropriate.

b. Staff

- Any breach of the staff acceptable use policy or staff code of conduct should be reported to the Headmaster.
- 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.
- Any disciplinary action will be taken in line with the Staff Disciplinary Procedure.

c. Searches

If an authorised member of staff has reasonable grounds for suspecting that a pupil / staff member is in possession of data or images that are inappropriate or against the terms of use, s/he is entitled to conduct a search.

Those authorised to conduct a search are as listed below:

- The Headmasters
- The Deputy Heads
- Online Safety Committee members
- IT Manager
- The Assistant Heads: Head of Upper School, Head of Middle School, Head of Lower School and the Assistant Head – Pastoral.
- Housemasters/Housemistresses (Senior School)
- Phase Leaders (Junior School)

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.

The authorised member of staff should take care that, where possible, searches do not take place in public places such as an occupied classroom or a corridor, in order to protect the privacy of the individual being searched; ~~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.

See **Appendix 1** for **guidance on what to do in the event of discovering content containing indecent images of children or criminally obscene adult content**

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 users 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.

6. Specific areas of responsibility:

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

The Headmaster and the Headmaster of the Junior School have an obligation to draw up strategies and procedures which aim to prevent Online Safety incidents occurring amongst pupils and pupils**.**

- ~~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~~
- Discuss development of strategies and review current procedures with the School Leadership Team
- Ensure appropriate training is available to staff
- Ensure that the policies and procedures are brought to the attention of all staff
- Ensure that pupils are aware of the rules and expectations about online behaviour, including how to report concerns (eg cyberbullying)
- Ensure that parents/guardians have access to relevant policies via the website and on request.

Designated Safeguarding Lead (DSL):

Has the lead responsibility for online safety and understanding the filtering and monitoring systems and processes in place. They 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

The DSLs in the Senior and Junior Schools are responsible for:

- Making an annual report to the Education and Welfare Subcommittee ~~Headmasters~~ as part of the safeguarding review.
- Planning and arranging / delivering staff training on online safety.
- Triaging alerts from the Filtering and Monitoring service, and delegating their management to pastoral or safeguarding staff (including managing cases themselves)
- Day to day management of the policy and procedures, in liaison with the Head of IT and members of SLT.
- Overseeing support for pupils affected by online safety incidents, usually by delegating support to Housemaster/ Housemistress (Senior School) or Class Teacher (Junior School).
- Determining how best to involve parents/guardians in the solution of individual problems
- Referring cases where there is harm / a risk of harm to the pupil into Children's Services
- Reporting cases where a crime may have been committed against a child to the police

Online Safety Committee:

The Online Safety committee 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/Housemistress and Junior School Class Teacher informed of all incidents~~
- Meet termly to discuss and review current Filtering and Monitoring provision and other online safety matters.
- Meet in response to any serious online safety incident to review policy and procedures in the light of the incident.
- Consider and shape the school's response to new technical developments that impact pupil safety, such as the use by pupils and staff of AI tools
- Complete an annual audit of Filtering and Monitoring provision using an external auditing tool (eg from The Key)
- Discuss and review staff training needs
- Consider the particular needs of Boarding pupils, ensuring they have the capacity to make contact with family, while restricting access to potentially harmful online content.
- ~~Determine how best to involve parents/guardians in the solution of individual problems~~
- ~~Make an annual report to the Headmasters as part of the safeguarding review.~~

All Staff will:

- Know and implement the current policies and procedures
- Report any concern about or incident of ~~all incidences regarding~~ Online Safety ~~E-Safety~~, whether on-site or during an off-site activity.

Use IT services and devices safely and professionally, in line with the staff Code of Conduct, the staff Acceptable Use Policy and the Use of Artificial Intelligence Policy.

In line with Filtering and Monitoring requirements, ensure that pupils are using devices safely in lessons and other school activities by supervising their behaviour.

~~Staff have a dual responsibility: to use ICT safely and professionally themselves and to safeguard pupils' usage.~~

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 the relevant Acceptable Use Policy, the Staff Code of Conduct and the pupil Behaviour Policy ~~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 and other sanctions will also be considered, depending on the nature of the infringement. The exception to this is that 'Boarders Wi-Fi' (only accessible to boarding pupils) allows limited use of VPNs to access communications with family members and friends overseas where this contact would not otherwise be possible. This service is blocked overnight.

7. Links to other policies:

This policy links with:

- Anti-Bullying Policy
- Behaviour Policies
- Safeguarding Policy
- Staff Disciplinary Procedure
- Whistleblowing policy
- ICT Acceptable Use Policy (Staff)
- ICT Acceptable Use Policy (Pupils)
- Use of Artificial Intelligence Policy
- Prevent Policy
- Privacy 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/
https://www.gov.uk/government/publications/channel-guidance
Cyberbullying: Advice for headteachers and school staff 2014
Advice for parents and carers on cyberbulllying 2014
https://www.iwf.org.uk/resources/best-practice-guide

Reviewed and Approved	EWC	February 2024
Reviewed and Approved	Board	March 2025
Reviewed and Approved	EWC	February 2025
Reviewed and Approved	Board	March 2025
Reviewed	SLT	June 2025
Reviewed and Approved	EWC	May 2025
Reviewed and Approved	Board	June 2025
Reviewed	SWA/AF	January 2026
Reviewed and Approved	EWC	February 2026
To be Reviewed and Approved	Board	March 2026
Next Review		January 2027

APPENDIX 1

Discovery of content containing indecent images of children or criminally obscene adult content

The production and distribution of content that contains indecent images of children is an offence under the Protection of Children Act 1978 and the Sexual Offences Act 2003.

Being in possession of such content carries a penalty of up to five years in prison.

Making content, which includes downloading, storing and printing indecent images of children is an offence that carries a penalty of up to 10 years in prison.

If a user discovers content that contains indecent images of children, it is vital therefore that nothing is done that may lead to prosecution.

In the event of indecent images of children being discovered on a computer the following procedure should be followed:

1. **Lock the computer screen by pressing CTRL+ALT+DEL.**
2. **Do not print, copy, or email the content.**
3. **Do not look at any other content on the computer**
4. **If the images are on a PC, isolate the room where the PC is located. Lock a classroom if appropriate.**
5. **If the images are on a mobile device (eg laptop or ipad) lock the device and take it immediately to the Headmaster or Senior Deputy Head if onsite or as soon as practicable if offsite (see further details below).**
6. **Inform the Headmaster(s) and/or the Senior Deputy Head immediately.**

This applies to images produced from real world situations as well as those generated by AI tools.

There is a conditional defence, agreed by the Crown Prosecution Service and the Association of Chief Police Officers, that allows designated IT professionals to access content containing indecent images of children for the purposes of forwarding them on to the Police and the Internet Watch Foundation (the approved body that deals with criminal content online, specifically child sex abuse images and criminally obscene adult content). The Headmaster will nominate designated individuals if this support is needed. ~~At Royal Russell, the designated individuals are Mark Hayden, IT Manager, and Gerry Otti, Senior IT Network and Digital Technician.~~

If indecent images of children are found, in consultation with the Headmaster, the Police, and the IWF, one of the designated individuals will access the content and retrieve evidence for the purpose of analysis and possible legal action. Nobody other than those named individuals above should ever attempt to access or distribute material of this nature.

If a user discovers content and there is uncertainty about whether it may be illegal or not, it is better to assume that it is and to follow the procedure above. The legal framework emphasises the importance of reporting illegal content in a timely manner. It is better to assume the worst and to allow a full review to occur swiftly, than leave content unexamined.

Where staff have concerns that school or private email accounts have been compromised and illegal content has been sent, or a link to such content provided, please inform the Headmaster or the Senior Deputy Head immediately. They will authorise a process involving the designated IT professionals to investigate any concern and where necessary, report it to the Police and the IWF.

Content of an illegal nature that is accessed, stored, made, or distributed outside of school using school equipment is subject to the same legal conditions outlined above. Should users detect illegal content on mobile / portable devices provided by the school the equipment should be locked and

handed in to the IT Manager as soon as possible. Ideally, this should be within 12 hours of content being discovered. The Headmaster and/or the Senior Deputy Head should be telephoned and emailed immediately. Users should detail the nature of the content but not forward any content itself.

Where users discover content on the Royal Russell Network that contains what may be deemed to be criminally obscene adult material the procedure above should be followed.

Where staff accounts are found to have accessed or stored pornography via the Royal Russell School Network that does not contain indecent images of children, this will be interpreted as a breach of the ICT Acceptable Use Policy and the Staff Code of Conduct. Disciplinary procedures and dismissal may ensue.