



RADLEY

Filtering and Monitoring Policy

June 2026

This policy should be read in conjunction with Keeping Children Safe in Education, the [Safeguarding Policy](#) and the [Use of IT Policy](#)

Aims

The use of technology presents serious challenges and risks to children and adults, both inside and outside school.

Radley College aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

We acknowledge that while filtering and monitoring are essential components of our school's online safety strategy, they form only part of a broader, proactive approach and that there are particular dangers in a boarding context. Pupils and adults may access the internet through personal devices and mobile data networks, which bypass school filtering systems. In addition, devices brought into school may already contain preloaded harmful content. Where such concerns are identified, appropriate and proportionate action will be taken to safeguard pupils and uphold our duty of care.

The main safety issues, highlighted in KCSIE, are broadly categorised into the following areas of risk:

- Content (exposure to inappropriate content, e.g. pornography). This includes content created with Generative AI.
- Contact (harmful online interaction)
- Conduct (online behaviour)
- Commerce (gambling, etc.)

All decisions about filtering and monitoring should be made considering:

- The context of the school.
- The digital resilience of pupils in the school and the risk profile of specific groups such as those with SEND and EAL.
- The fact that most pupils are likely to have additional devices which do not use the school network. Therefore, there is a need for education (through the development of digital competency skills in both PSHE and the Shell Computer Science course) as well as restriction.
- The balance between restriction and freedom of enquiry. Systems should block harmful and inappropriate content but not unreasonably impact teaching and learning.

The standards listed in [Meeting digital and technology standards in schools and colleges](#) must be met.

College Issued Pupil Devices

College issued pupil devices are monitored in term time only, they are not actively monitored by the College out of term time. However, parents are able to view the activity of their child's browsing and set alerts should they wish. They have the ability to increase the severity of the

filtering restrictions but not weaken them and they can pause the internet on that device. All of this is achieved through the College's filtering system Securly and its associated app which parents can sign up to.

Network Security and VPN Usage

The College network is configured to provide a secure online environment for all users. Robust firewall and security systems operate continuously to safeguard against harmful content, cyber threats, and malicious activity. When connected to the College's Wi-Fi, users can be assured that appropriate measures are in place to protect data integrity and confidentiality.

The use of Virtual Private Networks (VPNs) on the College network should be avoided. While VPNs are often marketed as security tools, they can introduce vulnerabilities, including exposure to cyberattacks and misuse. Free VPN services, in particular, may compromise privacy by monetising user data through third-party sharing.

VPN usage interferes with the College's ability to maintain network protections and monitor activity for safeguarding purposes. It may also impede technical support in the event of account compromise and cause operational issues, such as reduced network performance or restricted access to essential educational platforms.

To ensure a safe, reliable, and well-managed digital environment, we ask that all users refrain from using VPNs when connected to the College network.

Roles

Council has overall strategic responsibility for filtering and monitoring.

Assurance that the standards are being met should be provided by:

- The Designated Safeguarding Lead (DSL) who is a member of the College Management Team, and
- The Designated Safeguarding Governor (DSG)

The DSL and DSG, aided by the Director of Digital Strategy and the IT team, will:

- Review the effectiveness of provision
- Make and record decisions about what is allowed and what is not
- Review logs
- Follow up on any legal or safeguarding concerns
- Ensure staff are appropriately trained and kept up to date with current trends in social media usage (language and emojis)

Annual Review

There will be a review of filtering and monitoring conducted by the DSL, which will cover:

- Related safeguarding or technology policies and procedures
- Roles and responsibilities
- Training of staff

- Curriculum and learning opportunities
- Procurement decisions
- How often and what is checked
- Monitoring strategies

This review should be conducted at least annually, or when

- A safeguarding risk is identified
- There is a change in working practices, like remote access or the way in which personal devices access our network
- New technology is introduced

The annual review will inform updates to the Safeguarding policy which are reported and approved at the summer term Council meeting.