Reigate Grammar School Group

Online Safety Policy

Including Early Years Foundation Stage

Policy Author:	Brendan Stones, Deputy Head and Sarah Arthur, Deputy Head
Date Reviewed:	June 2025
Next Review Due:	June 2027
Date Approved By Governing Body:	16 June 2025
Next Review by Governing Body Due:	June 2026

This Online Safety Policy applies to all members of the school community (including staff, students, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed)

Objectives

- Safeguard children and young people from online risks, following the **4Cs framework**:
    - Content: *being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.*
    - 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: *online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual 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.*
- Establish clear expectations for safe and responsible technology use.
- Ensure effective governance, technical systems and educational provision.
- Promote digital resilience, cyber awareness and AI literacy.
- To ensure that Students are appropriately supervised during school activities
- To promote responsible behaviour with regard to online activities
- To reduce risk and build resilience, including to radicalisation, with particular attention to safe use of technology and the internet

This policy should be read in conjunction with the following:

- **Safeguarding Policy**
- **Behaviour Policy**
- **Staff Code of Conduct**
- **Online Behaviours (Staff) Policy**
- **Online Behaviours (Students) Policy**
- **Online Risk Assessment**

Policy development, monitoring and review

The Online Safety Policy has been developed in conjunction with the Headteacher, Deputy Head teachers, Online Safety Lead, DSL Team, Section Heads and Heads of Year, IT Team, Students, Parents and Governors though a range of formal and informal means.

The impact of the policy is monitored through a range of formal and informal means, for example:

- Logs of reported incidents
- Filtering and monitoring logs
- Surveys and voice activities with Students, parents and staff

The policy will be reviewed annually by the Online Safety Group, DSL and governors.

Reviews will take account of safeguarding incidents, emerging risks, changes in technology, DfE expectations and stakeholder feedback.

Policy updates will be communicated to all staff, students and parents.

Responsibilities

Headmaster

The Headmaster has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day oversight and management will be delegated to those with specific responsibilities related to e-safety.

The Headmaster, Designated Safeguarding Lead (DSL) and Deputy DSLs should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Headmaster for ensuring that the Designated Safeguarding Lead and Online Safety Lead, IT technical staff and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy:

- This review takes place through the Designated Safeguarding Governor by:
    - Having regular meetings with the Designated Safeguarding Lead/Online Safety Lead
    - regularly receiving (collated and anonymised) reports of online safety incidents
    - Checking that provision outlined in the Online Safety Policy is taking place as intended
    - Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually
    - reporting to relevant *governors group/meeting*

Designated Safeguarding Lead(s)

- hold the lead responsibility for online safety, within their safeguarding role responsibilities
- be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- attend relevant governing body meetings/groups
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out

Online Safety Lead(s)

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policy and procedure
- promote an awareness of and commitment to online safety education/awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/students
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by students) with regard to the areas defined In Keeping Children Safe in Education (KCSIE):
    - content
    - contact
    - conduct
    - commerce

Curriculum Leads

Curriculum Leads will work with the DSL Team and Online safety Co-ordinator to develop a planned and coordinated online safety education programme.

This will be provided through:

- drop down days
- PHSE and SRE programmes

- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week.*

Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood the Online Behaviours (Staff) Policy
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with students, parents, carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements).*
- they immediately report any suspected misuse or problem to a member of the DSL Team for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure students understand and follow the Online Safety Policy and Online Behaviours (Students) Policy, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the school's Online Behaviours (Staff) Policy with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the students in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Team

The IT Team is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges.
- there is clear, safe and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to a member of the DSL Team for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated.

Students

- are responsible for using the school digital technology systems in accordance with the **Online Behaviours (Students) Policy**
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- making available a copy of Online Behaviours (Students) Policy
- publish information about appropriate use of social media relating to posts concerning the school.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Professional Standards

- There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.
- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Students will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend students' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard students in the digital world
- describes how the school will help prepare students to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents
- is supplemented by a series of related Online Behaviours Policies

- is made available to staff at induction and through normal communication channels (to be described)
- is published on the school website.

Acceptable Use

The school has defined what it regards as acceptable use/unacceptable use and his is shown in the following documents:

- **Behaviour Policy**
- **Staff Code of Conduct**
- **Online Behaviours (Staff) Policy**
- **Online behaviours (Students) Policy**

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Deputy DSL, Online Safety Lead and other responsible staff with appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures. This may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged via the schools electronic logging system CPOMS. Staff should be aware that incidents might include risks such as:
    - peer on peer abuse
    - sexting
    - pornography

- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions as relevant
- learning from the incident (or pattern of incidents) will be provided the relevant members of the school community

Responding to student and staff actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Use of Artificial Intelligence in School

As Artificial Intelligence continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and students about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and students will, as always, be at the forefront of our policy and practice.

More detail on the schools approach to AI can be found in the Online Risk Assessment

Online Safety Education Programme

Staff

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding, data protection and cyber-security training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Online Behaviours Policies. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of involved in technology/online safety /safeguarding.

Additional training for the Safeguarding Governor, where required, will be made available to allow them to understand the school's filtering and monitoring provision so that they can fully participate in checks and reviews.

Families

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc

- the students – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by students leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform, high profile events/campaigns e.g. Safer Internet Day
- Sharing good practice with other schools in clusters and or the local authority, Trinity Group and HMC

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection

The school filtering and monitoring provision is agreed by senior leaders, online safety leads, the Director of IT and the Network Manager Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT Team will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead, the Online Safety Lead and the IT Team.

Checks on the filtering and monitoring system are carried out by the IT Team with the involvement of a senior leader, the Designated Safeguarding Lead and in particular when a safeguarding risk is identified or there is a change in working practice or a new technology is introduced using SWGfL Test Filtering.

While the school maintains robust filtering and monitoring on its own networks, it acknowledges that personal devices using 3G, 4G, or 5G connections may bypass these protections. This creates potential safeguarding risks, including exposure to inappropriate content, online grooming, peer-on-peer abuse and sexting. The school educates students, staff and parents about these risks and requires students to follow Online Behaviours (Students) Policy regardless of whether devices are connected to the school network or mobile data. Incidents relating to unsafe or harmful use of mobile data will be treated in line with the school's safeguarding and behaviour policies.

Filtering

- The DSL, online safety leads, IT Team and link Governor are responsible for ensuring these standards are met.
- the school manages access to content across its systems for all users and on all school devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Safeguarding Team to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. Members of the DSL Team, IT Team and Online Safety Leads are involved in the process and aware of the findings. (the school uses SWGfL Testfiltering.com to carry out these checks).
- Devices that are provided by the school have school-based filtering applied irrespective of their location.

- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/students, etc.)
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice

Monitoring

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users. These systems include Senso, Smoothwall Monitor as well as regular IT Team checks of irregular patterns of behaviour.

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead or DSL Team members. All users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead and technical staff. The results of the review will be recorded and reported as relevant. ·
- Monitoring enables alerts to be matched to users and devices.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges. Responsibility for technical security resides with SLT who may delegate activities to identified roles.

Mobile technologies

The school Online Behaviours Policies for staff and students outline the expectations around the use of personal mobile technologies:

- **Online Behaviours (Staff) Policy**
- **Online Behaviours (Students) Policy**

Digital and video Images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance/policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those students whose images must not be taken/published.
- students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- permission from parents or carers will be obtained before photographs of students are taken for use in school or published on the school website/social media.
- images will be securely stored in line with the school retention policy

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. Please see the Data Protection Policy for more information.

Cyber Security

The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage."

With respect to cyber security:

- the school has reviewed the DfE Cyber security standards for schools and colleges and meets these standards
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff receive training on the common cyber security threats and incidents that schools experience
- the school's education programmes include cyber awareness for students
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, students; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.