REIGATE GRAMMAR SCHOOL

E-Safety Policy

ISI Code:	E-Safety Policy
Policy Author:	Brendan Stones, Deputy Head Nick Lobb, E-Safety Co-ordinator
Date Reviewed:	June 2023
Next Review Due:	June 2025
Date Approved By Governing Body:	19 June 2023
Next Review by Governing Body Due:	June 2025

Objectives

- To ensure that pupils are appropriately supervised during school activities
- To promote responsible behaviour with regard to e-based 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 Safeguarding Policy, Behaviour Policy and the Staff Code of Conduct (Safeguarding Children, Protecting Staff).

The Headmaster and SLT

The Headmaster and SLT have 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 (DSLs) and Deputy DSLs should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Responsibilities

Whilst it is the responsibility of all staff to be alert to any issues of e-safety and to promote safe use of all modern technologies, there are several people with specific responsibilities for e-safety: The Bursar; Head of Computing; IT Manager; E-safety co-ordinator; Head of PSHEE; Heads of Section; and the Designated Safeguarding Leads. The E-safety coordinator will take a lead in ensuring that:

- Staff record and act on e-safety incidents;
- Keep the Headmaster informed of concerns relating to e-safety incidents;
- provide/arrange for staff training;
- liaise with school technical staff;
- liaise with the Headmaster, SLT or pastoral team on any investigation and action in relation to e-incidents;
- provide information to parents i.e. digital bulletin, parent forums;
- Oversee the pupil Digital Committee and liaise with the Head of PSHEE to develop a robust e-safety curriculum; and
- advise on e-safety policy review and development.

The **IT Manager** (who is responsible to the Deputy Head) will:

- be responsible for the IT infrastructure and see that it is not open to misuse or malicious attack;
- ensure that users may only access the networks and devices through an enforced password protection policy, including regular enforced changes;
- keep up to date with e-safety technical information in order to carry out their role;
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse;
- implement any agreed monitoring software/systems. See Appendix 1.

Teaching and Support Staff will:

- maintain awareness of school e-safety policies and practices;
- report any suspected misuse or concern connected with the pupils to the relevant Head of Year, or if it is a potential child protection issue, to the DSLs;
- report any suspected misuse by staff directly to the Headmaster;
- ensure that all digital communications with pupils/parents/carers/fellow staff are on a professional level and conducted on school systems;
- recognise e-safety where relevant in teaching activities and curriculum delivery;
- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- monitor the use of digital technologies (including mobile devices, cameras etc.) during school activities

- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches i.e. they should report this to one of the DSLs.

The **Head of PSHEE** and **Pastoral Team** will:

- plan a PSHEE curriculum which ensures that pupils are made aware of issues surrounding e-safety, for example, cyberbullying; safer social networking; managing your online profile/reputation.
- plan assemblies, tutor time and PSHEE which include reference to the risk posed by adults and young people who use the internet and social media to bully, groom and radicalise.

Pupils:

- are responsible for using school digital technology systems in accordance with the school acceptable use policy;
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking/using of images and cyber-bullying;
- will understand that the e-safety policy will include actions outside of school where related to school activities.

Parents/Carers:

- will be advised of e-safety policies through parents' evenings, newsletters, letters, school website etc.;
- will be encouraged to support the school in the promotion of good e-safety practice;
- are invited to give consent for their son/daughter's image to be used in school publications;
- are invited to relevant parent forums/workshops.

Child Protection

The DSLs should be aware of e-safety issues and in particular of the implications that may arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate contact online with adults/strangers
- potential or actual incidents of grooming – sexual exploitation
- cyber-bullying
- exposure to radicalisation

The effectiveness of this policy will be evaluated by SLT.

Appendix 1: Monitoring Computer Usage at Reigate Grammar School

All monitoring of school owned/provided systems will take place to safeguard members of the community. The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

Impero

Impero is our management software system, which monitors computer usage, provides e-safety, power management and remote control support as well as many other features. This includes monitoring of potential bullying, child protection, and radicalisation issues.

> *"Impero Education Pro is designed to keep students safe in the online environment. Viewing unsuitable content, giving out personal information, accessing indecent images, cyber-bullying, grooming, identity theft – the risks go on. With key word detection and the use of blocks and filters, Impero's digital classroom management software incorporates e-safety for schools and ensures acceptable boundaries can be imposed. Real-time alerts and close monitoring will highlight violations, usually proving enough of a deterrent to prevent these instances occurring in the first place."*

Impero at RGS

Impero Education Pro provides site wide system monitoring. Impero monitors student activity on school owned laptops and PCs against keyword libraries developed in partnership with nationally recognised e-safety organisations:

- https://www.imperosoftware.co.uk/corporate/e-safety-partners/

Further details of Impero's capabilities and monitoring features can be found at:

- https://www.imperosoftware.com/uk/products/education-pro/online-safety/

Smoothwall

Monitoring internet and email access using Smoothwall. This is a scalable web and spam filter solution which ensures compliance, student safety, flexible policies and reporting. This filters and records internet searchers against a keyword list as well as holding and blocking blacklisted web addresses. Keyword lists are reviewed and updated regularly by IT and safeguarding leads.

- To learn more about Smoothwall please visit: Firewall | Smoothwall® | Digital safeguarding solutions
- Smoothwall's privacy policy can be found here: https://www.smoothwall.com/education/privacy-policy/#privacyschools
- Smoothwall produces a daily internet filter report that is reviewed by members of the DSL team.

Smoothwall Monitor

Smoothwall Monitor is used to monitor activity on school owned devices and has a sophisticated real time reporting system to appropriate staff members.

Senso

The Senso system monitors Teams chat activity on any device. Senso has a sophisticated real time reporting system to appropriate staff members.

Monitoring Email access using Microsoft Threat Protection

This is a scalable Spam Filter solution, which ensures compliance, student safety, flexible policies and reporting.

Monitoring Devices connecting to the Wi-Fi Network using Ruckus

Ruckus is a complete Wi-Fi system providing an enterprise grade wireless network with bespoke Wireless Access Points which interface with its Zone Director software allowing us to constantly monitor and support the Wi-Fi services at RGS.

Testing

The School IT system has appropriate levels of filtering to ensure children are safe from terrorist and extremist material and social media accounts when accessing the internet and the system is regularly checked and tested.

Responsibility for monitoring

System monitoring though Impero, MS Threat Protection, Lightspeed, web filter monitoring is by the DSL team and will be recorded and escalated as appropriate.