Online-Safety Policy

Date Agreed by the Governing Body	November 2022
Date to be reviewed	November 2023
Date of last review	November 2021
Governors Committee accountable for review	Education
Senior Leadership Team member accountable for review	JIS

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
4. Educating pupils about online safety 7
5. Educating parents about online safety 9
6. Cyber-bullying 9
7. Acceptable use of the internet in school 11
8. Pupils using mobile devices in school 11
9. Staff using work devices outside school 11
10. How the school will respond to issues of misuse 12
11. Training 12
12. Monitoring arrangements 13
13. Links with other policies 13
Appendix 1: Acceptable use agreement (pupils and parents/carers) ..... **Error! Bookmark not defined.**
Appendix : 2 Acceptable use agreement (staff, governors, volunteers and visitors) ..... **Error! Bookmark not defined.**
Appendix 3: online safety training needs – self audit for staff ..... **Error! Bookmark not defined.**
Appendix 4: online safety incident report log 14

1. Aims

AT RGS we aim to:

- 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 (which we refer to as 'mobile phones')
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Establish clear mechanisms to identify, intervene in and escalate an incident, where appropriate
- Ensure that risks are clearly identified, assessed and mitigated in order to reduce any potential harm to students and staff, and any liability for the school.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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 scam

2. Legislation and guidance

This document provides a guide for adults working in our school about acceptable and desirable conduct to protect both adults and students. It also includes guidance for students and parents on Online Safety issues. This policy is based on the Department for Education's (DfE) statutory safeguarding guidance. It refers to and complements other policies and

guidance at The Royal Grammar School with which all staff, volunteers and visitors must be familiar and work in accordance to. The policies include in particular:
Keeping Children Safe in Education 2022 and as amended from time to time and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
    - It also refers to the DfE's guidance on protecting children from radicalisation.
    - *Working together to safeguard children (July 2018 brief update Feb 2019).*
    - *What to do if you're worried a child is being abused (March 2015)*

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL)

The governor who oversees online safety is currently Sarah Abbas (Safeguarding Governor)

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and ADSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

In addition, the Online Safety Officers (Named DSL and ADSLs) will:

- Keep up to date with the latest risks to children using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Senior Team.
- Advise the Senior Team and governing body on all significant online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Ensure any technical online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose.
- Make themselves aware of any reporting function with technical online safety measures, i.e. Internet filtering reporting function.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School Behaviour Policy
- Passwords are applied correctly to all users.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School Behaviour Policy
- Being aware of the latest guidance in KCSiE (Sept 2022) in relation to electronic devices and Searching, Screening and Confiscation Advice for Schools July 2022.
- If staff search or confiscate devices following DFE guidance. Staff must not **intentionally** look at nude or semi-nude images, or copy, print, share, store or save such images, and that these must be referred immediately to the DSL/ADSL.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Knowing the name of the Designated Safeguarding Lead (Mr David Durning– Assistant Head) and the Additional Designated Safeguarding Leads (Mr Scourfield, Mrs Herath, Mrs Barry (Matron) & Mr T Fossey).
- Creating a safer online environment
- Giving everyone the skills, knowledge and understanding to help children and young people stay safe online.
- Inspiring safe and responsible use and behaviour

- Use of mobile phones both within school and on school trips/outings
- Use of camera equipment, including camera phones
- What steps to take if you have concerns and where to go for help
- Ensuring any Online Safety incident is reported to the Online Safety Officers within 24 hrs so that appropriate action can be taken. If staff are unsure, the matter should be raised with the Online Safety Officers who will make appropriate decisions.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- play the most important role in the development of their children and as such the school will support parents in accessing resources to acquire the skills and knowledge they need to ensure the safety of children outside the school environment.
- understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such all parents will sign the Acceptable Use of ICT Systems (including Remote Learning addendum) and Learning Gateway for Students before their son can be granted any access to the school network, ICT equipment or services. All parents receive guidance on photography or recording of images of RGS students. A list of students whose parents have indicated that they would not like their son's image recorded will be held by the Admissions Office and online safety officers.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

- The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use of ICT Systems and Learning Gateway for Students (including RGS

Remote Learning Policy), the School Rules, the Behaviour Policy, the Valuables Policy and the iPad Agreement **(All available on Sharepoint).**

- All students sign and agree to the Use of ICT Systems and Learning Gateway for Students before being granted any access to the school network, ICT equipment or services. This includes ??
- Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the School Behaviour Policy.
- Online Safety is embedded into the curriculum – students will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.
- All students will be fully aware of how they can report areas of concern whilst at school or home.

Pupils will be taught about online safety as part of the curriculum:

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website School Policies via website .This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors and indeed Class teachers where appropriate will discuss cyber-bullying with their teaching/tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHCE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The School also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the School will follow the processes set out in the School Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The School's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the School Complaints Procedure.

7. Acceptable use of the internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the School's terms on acceptable use if relevant.

Use of the School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the Acceptable Use Agreements in appendices 1 and 2.

8. Pupils using mobile phones in School

Pupils may bring mobile phones into School, but are not permitted to use them during the school day.:

Any use of mobile phones in School by pupils must be in line with the Acceptable Use Agreement (see appendices 1).

Mobile devices such as iPads can only be used when specific permission is given by subject staff, they are used regularly as a teaching tool

Any breach of the Acceptable Use Agreement by a pupil may trigger disciplinary action in line with the School Behaviour Policy, which may result in the confiscation of their device and potentially a further sanction in line with the School Behaviour Policy.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the School's Terms of Acceptable Use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT department.

10. How the School will respond to issues of misuse

Where a pupil misuses the School's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the School's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/Staff Code of Conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The School will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police and or LADO.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and ADSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Acceptable Use of ICT Systems Policy and Internet Safety
- Additional Boarding Guidance papers to boarding staff and students.
- Anti-Bullying Policy
- Behaviour Policy
- Child Protection Policy
- Complaints procedure
- Equal Opportunities and Race Equality Policy
- Guidance on Photography and Recording images of RGS students
- Health and Safety
- Mobile Phone Guidance
- Peer on Peer Abuse Policy.
- Preventing Radicalisation Policy
- Privacy Notices for Pupils, Parents and Staff
- PSHE and Relationships Policy

- Staff Code of Conduct. 'Guidance for Safe Working Practices for the Protection of Children and Staff'
- Staff Handbook
- Valuables Policy

Appendix 1 online safety training needs – self audit for Online safety

Appendix 2: online safety incident report log

Appendix 1

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**