Online Safety and Acceptable Use of Smart Devices Policy

Incorporating the Acceptable Use of IT Policies, the Internet Access Policy and the pupil use of mobile devices (including iPads) policy

The Royal Grammar School Worcester
September 2024

Policy Statement

This policy applies to the four schools comprising RGS Worcester (RGSW, "the School" or "the Schools"), being RGS Worcester, RGS The Grange, RGS Dodderhill and RGS Springfield.

This policy applies to all relevant digital devices, i.e. not just desktops and laptops, but also smartphones, tablets, headsets and watches where applicable. The policy applies to both School and privately-owned equipment brought on site by either pupils, staff or third parties, as well as School and privately-owned equipment used to access RGSW services and data.

The Governors and Head Teachers of the four RGS Worcester Schools, believe in the educational benefits that can be offered to pupils through the correct and appropriate use of technology. However, it is acknowledged there is a need to address the dangers and raise awareness of potential abuses of technology. Good planning and management at RGSW will ensure appropriate and effective staff and pupil use.

This policy is designed primarily to safeguard pupils, but also to provide guidance for adults in positions of responsibility. It applies to all members of the RGSW community, including pupils, teachers, support staff, visitors, volunteers and temporary staff and Governors. It is not limited to the school network; it is designed to cover all aspects of Online Safety that may impact on the school community.

The safe and appropriate use of technology is not a standalone issue. This policy should be read in conjunction with a number of related policies, including, but not limited to;

- The RGSW Use of Images Policy.
- RGSW Safeguarding policies.
- Senior School and Prep School sectional handbooks.
- RGSW Data Protection Policies
- RGSW Cyber Security Policy

Staff should also abide by the contents of the Staff Digital Devices Policy and familiarise themselves with the contents of the email etiquette policy.

As with all aspects of safeguarding and our strong focus on pastoral care, all members of staff have a responsibility to promote awareness and compliance with the terms of this policy.

Roles and Responsibilities

The Head Teachers and Governors will ensure the Online Safety and Acceptable Use of Smart Devices Policy and related policies are implemented. These policies will be reviewed during the course of each academic year, or post any specific technological developments by The IT Department, prior to being endorsed by a member of the Governing Body.

Communicating the contents of these policies

These policies will be published both internally on our Intranets, as well as externally on the public RGSW website. (http://www.rgsw.org.uk) Their contents will be broadcast to both pupils, staff and parents at least annually to raise awareness of the responsibilities of all respective parties.

On joining the Senior School pupils will be asked to acknowledge their awareness of, and agreement to abide by the related pupil IT codes of conduct, including the use of iPads and mobile devices. Similarly, staff will be asked to acknowledge their awareness of, and agreement to abide by both this policy and related staff policies and etiquettes.

Education and Awareness

The School considers itself to have a central role in educating pupils, parents and staff in issues that may affect them in this area. The School provides a programme that raises awareness of technical and behavioural aspects of safety for pupils, including topics such as advice on grooming and radicalisation, exposure to material that is not appropriate to their age, the sharing of personal information, their online footprint, cyber bullying, sexting, Artificial Intelligence as well as the use of social media and digital communication in general. This is delivered throughout the curriculum generally, and specifically in PSHCE and Computing and IT periods, as well as assemblies. The programme is designed to deliver information and explore issues at a level appropriate to the age of the pupil, and certain topics will be revisited at appropriate points in each pupils development.

This programme also includes sessions run annually, at all four RGS Schools for parents/guardian's, highlighting both the material that is delivered to our pupils, but also to assist and educate parents, so they are better informed to support their children use technology appropriately.

This policy will be published both internally on our Intranets, as well as externally on the public RGSW website. (http://www.rgsw.org.uk) It's contents will be broadcast to both pupils, staff and parents at least annually to raise awareness of the responsibilities of all respective parties.

On joining the Senior School pupils will be asked to acknowledge their awareness of, and agreement to, abide by the related pupil IT code of conduct, including the use of iPads and mobile devices. Similarly, staff will be asked to acknowledge their awareness of, and agreement to abide by both this policy and the Use of Staff Digital Devices Policy.

How will staff, pupils and parents be kept informed?

Staff

It is important that Staff feel prepared for Internet use and agree with the school IT usage Policy. Staff should be given opportunities to discuss the issues and develop good teaching strategies. Staff receive training on, and are made aware of the relevant IT policies prior to being issued with their RGS account UserID credentials and/or receiving school equipment for their professional use. They also receive training and guidance both as part of mandatory Safeguarding training, and the INSET programme. New staff receive suitable training and guidance as part of their induction.

Parents

There may be a gap between some parents' awareness of safety issues, and the technical proficiency of their children. Therefore, the school provides information and guidance to help bridge this gap through a variety of means, including briefings at Parents' Evenings, letters, newsletters and the Parents' Portal. (portal.rgsw.org.uk)

Should parents have any concerns over, or wish to seek guidance on, any aspect of Online Safety or the use of technology, they are encouraged to contact their child's Form Tutor or Head of Year in the first instance. In the event of more serious issues Parents are invited to contact the Director of Innovation - John Jones, or at the Senior School the Senior Teacher (Pastoral and Welfare) Mrs Sofia Nicholls, at RGS The Grange the Head of Computing - Matthew Warne, at RGS Springfield the Headmistress, Laura Brown and RGS Dodderhill the Headmaster - Tom Banyard. RGS believes that communication between home and school is vital in the establishment of good use of technology safety principles and practice.

Should parents have concerns that their child has been subjected to attempts at sexual grooming, radicalisation, or other inappropriate online contact, they should contact the relevant Designated Safeguarding Lead for the relevant school as a matter of importance. These are the Senior School, Assistant Head (DSL) – Mrs Sofia Nicholls, at RGS The Grange, the Deputy Head - Mrs Wendy Wreghitt, at RGS Dodderhill - the Deputy Head, Ms Sarah Clay and at RGS Springfield the Headmistress - Laura Brown. Where appropriate the DSL's will liaise with outside agencies, such as social services, the police and possibly also the CEOP (Child Exploitation and Online Protection) service, (details of which can be found at www.ceop.police.uk)

Should parents wish to discuss any other aspect of online behaviour, such as possible online gaming addiction, or concerns about the amount of time spent online, they should similarly contact any of the relevant staff as a matter of importance.

Pupils

Pupils receive training across our Family of Schools both as part of their curriculum Computing lessons and their PSHCE classes. Theme based assemblies also contribute to the effort to raise awareness at appropriate times during the year

Rules promoting safe and responsible use of technology will be posted on appropriate, easily accessible school digital notice boards and the School intranet.

The Acceptable Use Statement or Rules for Responsible Internet Use may appear as posters in areas where school computers are located.

The RGSW Network

RGSW is responsible for ensuring the School Network is as safe and secure as possible, and undertakes to filter content, denying access to material that might prove offensive, inappropriate, promote radicalisation, be illegal or harmful.

These filters are reviewed regularly, but the School cannot guarantee that such material is always inaccessible. All parties should be aware that both staff and pupils are readily able to access the Internet via either a 3G, 4G or 5G unfiltered service, provided by a mobile phone provider, and propagate that access by creating a hotspot. Such activity is deemed highly inappropriate. The School cannot accept liability for any material accessed, or any consequences of this type of internet access.

Students are given training on how to keep safe online, and what to do should they find inappropriate material. They are expected to adhere to the Online Safety and Acceptable Use of Smart Devices Policy, as published in the Appendix of this document.

All users are provided with a username and password, and will have clearly defined access rights to the school IT systems. The School will monitor the use of communications and online behaviour for all users of the system in order to best ensure that the online environment remains both safe and secure.

It is the responsibility of all staff to adhere to the Safeguarding policies, and these apply just as much to the use of IT systems, either those in the School Network, or outside of it. The three principles of ***Prevention, Protection and Support*** should determine any action taken by a member of staff.

If members of staff wish to seek guidance on any aspect of Online Safety, they should consult the Deputy/Assistant Head (Pastoral) or the Director of Innovation.

Why write an Internet access policy?

The Internet is an open communications channel, available to all. Applications such as Web Browsers, email, gaming and Social Networking/Media sites all transmit information over the wires, fibres, mobile and satellite links of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime, extremism and racism that would be more restricted elsewhere. Sadly email and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

RGSW needs to protect itself from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly an offence to hold images of child pornography on computers and to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". RGS can help protect itself by making it clear to users [pupils and staff] that the use of school equipment to view or transmit inappropriate material is "unauthorised". However, members of The Strategy Group are aware that a disclaimer is not sufficient to protect the school from a claim of personal injury and RGSW needs to ensure that all reasonable and appropriate steps have been taken to protect pupils and staff.

Why is Internet access important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and is of benefit for the pupils who show a responsible and mature approach. It should be noted that the use of the computer systems at RGS by both staff and pupils without permission, or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990. Pupils should be made aware of this by their form teacher/tutor, staff should be made aware of this by the relevant Headteacher or the Bursar as appropriate.

Internet use is a part of the RGS curriculum and a necessary tool for staff and pupils.
Internet access is an entitlement for students who show a responsible and mature approach to its use.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

CEOP's and Think U Know

RGSW has, and will continue to use, CEOP provisioned training materials when delivering eSafety sessions. These sessions will be lead by staff at RGS who have undergone appropriate accreditation from CEOP.

For more information visit - https://ceop.police.uk/ and https://www.thinkuknow.co.uk/

CEOP materials will therefore be used in PSHE and Computing and IT classes as well as Assemblies to advertise the risks as well as encourage both pupils and staff to behave responsibly.

During the course of each academic year we will continue our programme of education in this area which was initiated in 2006. We will reinforce the message and all staff and students will be made aware of the existence and purpose the CEOP Report Abuse button was added to both our Intranet and Internet sites in 2006 and will remain there.

Access to the Internet via a Third Party Carrier whilst on RGS Premises.

With the advancement of technology, access to the Internet via 3rd Party telecommunication systems is now both readily available, affordable and common place, for both pupils and staff. The School is not able to police such access via 'dongles' or 'smartphones' which allow access via mobile broadband but it is aware that pupils and staff may be able to access inappropriate material via such means. Therefore, to protect all parties concerned, the school reserves the right to examine any IP enabled device brought into school which has or could be connected to the School network. Approved anti-virus software must, where applicable, be installed on such devices.

Social Networking Sites

The use of Social Media has and will continue to increase. RGS advises all staff and pupils to use such systems in an informed manner. Any reference direct or indirect to either the School, or a member of staff, or a pupil at RGS must be carefully considered. The school reserves the right to ask for any comments/postings to be altered or removed that it considers inappropriate which make reference to any member of the school, or the School itself either directly or indirectly.

Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. Pupils are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School's code of conduct regarding the use of IT and technologies and behaviour online.

Access to social networking sites as a general rule is prohibited for pupils, although exceptions may be made where a suitable educational benefit can be cited by a pupil/member of staff to the Director of Innovation.

Staff are not permitted to communicate with parents, pupils or third parties in relation to any issue concerning RGS on any social networking site or related facilities. For example, direct communication via Facebook and Twitter is prohibited. The exception being via school or departmental accounts authorised for use by the Director of Innovation, in adherence with the published guidelines.

Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and pupils to remember that they are representing the School at all times and must act appropriately.

Accounts and Passwords

Pupils[1] and Staff, upon arrival, are issued with an RGS User ID and password, as well as an RGS Google Education Account. It should be noted that both accounts use the same password.

The RGS User ID gives access to the RGS WiFi system, RGS data store areas and RGS email accounts. It allows staff and pupils to log into RGS computers connected to the network in classrooms and various areas around the four schools.

[1] Pupils in Year Five upwards

Governors are also issued with an RGS UserID to allow them to access a series of RGSW resources to allow them to fulfil their function.

All users should be aware that they are solely responsible for all and any data held in their accounts, or any use of their accounts and related services, for example email. They should not share their account credentials with any third party, and if for any reason they believe the security of their account has been compromised should contact a member of the IT department as a matter of importance, such that the account can be locked and their password reset.

It is expressly forbidden for any user to access, or attempt to access any part, or use any RGSW IT service using another users credentials.

All devices brought into school, which a user wishes to connect to the RGSW network must be registered with our Mobile Device Management Solution (Jamf School). For further details please visit http://dlp.rgsw.org.uk/

Staff must connect their devices to the SSID (WiFi signal) call RGS Staff.
Pupils must connect their devices to the SSID (WiFi signal) call RGS Pupils.

The RGS Guest SSID is provided for visiting speakers. Time limited credentials will be provided when required through either Reception or a member of the IT technical services staff.

Users are expressly forbidden from bringing into school 'jailbroken' devices of any nature.

How will the risks of access to the internet be assessed and RGSW be sure access is appropriate and safe?

Some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a device The School cannot accept liability for the material accessed, or any consequences thereof.

While no technological solution can be 100% effective in guaranteeing safety when using the internet and related technologies, technology can help to minimise the risks to pupils, particularly when supported by a clear acceptable use policy and appropriate internet safety education.
Methods to quantify and minimise the risk will be reviewed annually by the Director of Innovation

Examples of e-safety issues RGS needs to be aware of, and protect its users from include;

Content
- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such images of child abuse

Contact
- Grooming using communication technologies, leading to sexual assault and/or child prostitution

Commerce
- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Culture
- Bullying via websites, social media, instant messaging or other forms of communication device
- Downloading of copyrighted materials e.g. music and films

Staff will need to ensure that access is appropriate to the user. Primary pupils will require protected access to the Internet. The oldest secondary pupils, as part of a supervised project, might need to access adult materials, for instance a set novel that includes references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying or harassment. Filtering will be adjusted as appropriate for the audience. For example a higher level of filtering will be enforced upon Students than will be the case for Staff.

Staff will check that the sites selected for pupil use are appropriate to the age and maturity of pupils;
The Strategy Group will monitor the effectiveness of Internet access strategies; access levels will be reviewed as pupils' Internet use expands and their ability to retrieve information develops; pupils will not at any time be permitted to buy anything over the Internet.

The Strategy Group will ensure that occasional checks are made on files to monitor compliance with the school's Internet Access Policy; staff who become aware that pupils are able to access any inappropriate material will be required to report the matter, in a timely fashion to the Computing and IT Department.

How will the security of RGSW Computing and IT systems be maintained?

The security of the whole system will be reviewed at least annually with regard to threats to security from Internet access;

Virus protection will be installed and updated regularly;

It will be the responsibility of the individual using any form of removable media (inc memory sticks) to ensure it has been virus checked prior to use;

A recognised hardware or software firewall will be installed, as approved by the Director of Innovation or IT Services Manager, and a subscription to the CyberNOT filter list [or equivalent] will be purchased and utilised. The system will provide facilities to enable different access levels for different groups of users at RGS, e.g., Staff, Senior School Pupils and Lower School Pupils. Where required a 'White List' will be used in place of a 'Black List', or Intranet only access may be permitted to certain Students.

Use of Email to send attachments will be reviewed from time to time, as will cloud based file sharing services;
Both staff and pupils bringing digital devices with WiFi capabilities into school will be required to use and adhere to the Mobile Device Management systems that have been implemented and are detailed here http://dlp.rgsw.org.uk/

How will Email be managed?

Because of the simplicity and low cost of email, care needs to be taken that the consequences to the school and the pupil of messages are appreciated. A major question is whether the responsibility for self-regulation should be delegated to individual pupils. It is difficult to control the content of email without compromising privacy. All email is processed through a spam and virus filter. Staff will be provided with regular Phishing and security training.

All staff and all pupils from Year 5 upwards will be provided with rgsw.org.uk email accounts.

Pupils will be taught how to use email as a communication tool.

Pupils and staff will be encouraged to ensure that communications with persons and organisations ensures appropriate educational use and that the good name of the school is maintained;

The forwarding of chain letters/emails will be banned;

Pupils with individual email accounts, will be held accountable for the use of that account;

In-coming and out-going email will be regarded as public, in so far as Staff and Pupils are reminded, they are provided with email accounts for school use. They should be prepared for any email they send or receive to be intercepted and read by an authorised employee of the school, or any such external agency as appointed by the school, including but not limited to law enforcement agencies. Staff authorised to intercept/read pupil email will include the Headteachers, DFO, Deputy Heads and Director of Innovation. Staff authorised to intercept/read Staff email will be limited to the DFO, or his appointed agent. The approval of the Chair of Governors must be sought to intercept/read the DFO's email, or any form of electronic communication.
email messages on school business to parents which contain sensitive and substantive information must be approved before being sent by a member of the appropriate SLT. Emails to groups of parents are to be made via the Parent Portal and Schoolpost system in line with the published protocols.

The use of third party email accounts by pupils at school will be discouraged and where possible blocked. [e.g. Hotmail.] Excessive social email use can interfere with learning and will be restricted.

For safeguarding purposes, staff are advised only to communicate with pupils electronically via the pupil's and member of staff's School email account, unless there are extenuating circumstances and a senior member of staff has been made aware.

Parents are asked only to communicate with staff via the member of staff's RGS email account.

Staff must tell their manager or a member of the respective SLT if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves. Staff are also required to equate themselves with the School email etiquette document.

Pupils should inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

Cyberbullying

RGSW has a zero-tolerance policy towards bullying, of all kinds. Cyberbullying, as with any other form of bullying, is taken very seriously. Information about specific strategies to prevent and tackle bullying are set out in the School's Anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the School will take it seriously. The school will act as quickly as possible to establish the facts. It may be necessary to examine School systems and logs, RGS or indeed pupil owned devices to determine the facts.

The incident will be recorded, and when appropriate be referred to third parties, for example the Police Service if deemed appropriate by the respective Headmaster/mistress. The school will provide support and reassurance to the victim, and if appropriate their family.

It will be made very clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the School will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to school's behaviour policy, and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their IT account access suspended to RGSW services.

Radicalisation

Radicalisation is the process by which individuals or groups come to adopt extreme views on political, religious and social matters, notably with the result of violent extremism. The School has a duty to protect children from extremist views, and to equip them with the ability to recognise, question and resist any attempts to radicalise during their formative years. RGSW educates Senior School pupils how to recognise these attempts as well as promotes critical thinking through the PSHCE curriculum. It is expected that anyone in the community brings to the School's attention any attempts to promote extremism.

How will we deal with suspected Sexting Incidents?

A mobile telephone/tablet/smartphone/laptop or other internet enabled device is the child's personal property. If a member of staff has been made aware of inappropriate images of a child or young person, they should inform the lead for the child protection in the school as the protection of the child or young person is paramount. A member of staff should not attempt to view the image(s) without having received authorisation from the appropriate DSL (Designated Safeguarding Lead), and when doing so should be in the presence of another senior member of staff. The image should not be forwarded to or saved on another device. However, the image should not be deleted until the appropriate DSL (under guidance from third parties as deemed necessary) advise it.

In line with child protection procedures and with the agreement of local police, the school should ask all of the young people in possession of the image to delete it. If the image has been forwarded outside the school environment contact the appropriate people and request that they follow the same steps. If the image has been uploaded to any website or social networking site, the School will contact the provider of the service to have it removed. All reputable social networking and content hosting sites will have robust terms of service under which the distribution of illegal materials is strictly forbidden. If RGS is unable to contact the providers of any websites hosting the image, they will report them to the Internet Watch Foundation at www.iwf.org.uk If the above steps do not resolve the situation, CEOP can be contacted at www.clickceop.police.uk

The parents of young people involved should be notified of the situation. The relevant DSL and the Director of Innovation and IT will discuss the "digital footprint" of the images and any images like it with the young people involved. RGS may also consider in-house counselling for the young people concerned, particularly if they were depicted in the image.

If a member of staff has reason to believe a pupil's phone/tablet/laptop may contain images of an inappropriate nature, the phone should be removed from the pupil and preferably as witnessed by the pupil be delivered to the appropriate DSL.

If the school suspects these images are published on the web it could need reporting to the IWF. Sexual photographic images of children under 18 are illegal. These are not child pornography pictures as some sites refer to them - they would be classed as child abuse.

As part of the PSHCE and digital safety programme, the ever-increasing dangers of sexting and transferring inappropriate images of young people will be highlighted as being not just inadvisable but illegal. It will be stressed how seriously RGSW will view such instances should they occur, and the potential sanctions they might attract.

How will complaints be handled?

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance it is possible that the issue has arisen through home Internet use or by contacts outside school. Transgressions of the rules by pupils could include minor as well as the potentially serious. Sanctions for irresponsible use will be linked to the School's Rewards, Behaviour and Sanctions Policy.

Responsibility for handling incidents will be given to the Director of Innovation and IT and the relevant Pastoral Deputy Head.

Parents and pupils will need to work in partnership with staff to resolve any issue;

As with drug misuse issues, there may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies;

If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the Computing and IT Department and blocked.

A pupil may have Internet access denied or restricted for a period, or their entire account suspended;

Denial of access could include all school work held on the system, including any examination work;

Any illegal/obscene material will be deleted.

All users of the school computer system are obliged to report inappropriate use of the system at any time by another user to the Computing and IT Department immediately.

The Digital Learning Programme - DLP

In November 2013 the Governors announced to parents the adoption of a Digital Learning Programme (DLP) at RGS. One of the main aspects of this programme will involve pupils bringing iPads to school. The rollout of the DLP is now fully complete. Every pupil from Year Five upwards who attends an RGS school, does so, complete with his or her iPad. Furthermore, every pupil in Years One to Four at RGS Springfield and RGS The Grange Schools is allocated an iPad for his/her dedicated usage whilst at school.

We recognise that because we have introduced technology so widely, our systems of protection and our digital safety arrangements need to be ever more robust.

A number of amendments to the IT infrastructure have taken place, including, at the time, the introduction of a Mobile Device Management (MDM) solution. Effective June 2014, all devices, regardless of who owns them (The School, staff or pupils) that connect to the RGS IT infrastructure are required to register with approved RGSW MDM solution, Jamf school. This will be referred to as 'registering with Jamf'. This will ensure that all parties are amply protected, as well as enabling the school to provision data, printing profiles and Apps. The pupils have drawn together a Pupil iPad Usage Policy, which forms an annex of this policy and becomes effective immediately. Further advice and assistance regarding the DLP is available from a dedicated resource introduced in September 2016 which offers support, tutorials and 'how to' guides to many aspects of the DLP can be found at the following address - http://dlp.rgsw.org.uk

Internet Access Policy

The computer system and related peripherals are owned by the School, and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The School's IT Policies, including the Acceptable Usage Policy incorporating the Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the School.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

All Internet activity should be appropriate to staff professional activity or the student's education, Irresponsible use may result in loss of Internet access, or the suspension of a user's IT account;

Access to the computer systems and network by both pupils and staff should only be made via the authorised account and password, which should not be made available to any other person;

If using RGSW WiFi, students may only use the RGS Student SSID (WiFi signal)

Activity that threatens the integrity of RGSW's Computing and IT systems, or activity that attacks or corrupts other systems, is forbidden.

All users are expressly forbidden from using, or attempting to use VPN services or applications to by-pass RGS filters whilst using RGS networking services.

Pupils are not permitted at any time to purchase anything over the Internet.

Users are responsible for all email sent and for contacts made that may result in email being received;

Use for personal financial gain, gambling, political purposes or advertising is forbidden;

Copyright and intellectual property rights of materials must be respected;

The use of Chat Rooms is not allowed.

During the school day, pupils are not permitted to access web sites, play games, use Social media or Instant messaging unless the activity is linked to a lesson, and has been specifically authorised by a member of staff. Posting anonymous messages and forwarding chain letters is forbidden;

As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;

Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

Information such as home addresses, telephone numbers or any other personal details must not be transferred over the Internet without parental permission.

Any unpleasant material or messages received must be reported to a member of staff.

The school reserves the right to examine any computer/smartphone brought into school which has or could be connected to the School network. Approved anti-virus software must where applicable be installed on such devices.

Pupils must abide by the Use of iPads and Mobile Devices rules.

Rules for Responsible IT and Internet Use
Prep Schools & Lower School Version

- The School has installed computers with access to the Internet as an educational resource. These rules will keep you safe and help us be fair to others.
- I will only access the system with my own login and password, which I will keep secret. I will ask permission before using the Internet in class;
- I will not access or attempt to access other people's files;
- I will use the computers for school work and homework only;
- I will only email people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not buy anything over the Internet;
- I will not use Internet Chat Rooms, or social media whilst at school;
- I will not use VPN services or 3G, 4G, 5G connectivity
- I will not give my home address or telephone number, or arrange to meet someone, unless my parents have given permission;

- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;
- I understand that the School may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.
- The school reserves the right to examine any computer/smartphone brought into school which has or could be connected to the School network. Approved anti-virus software must where applicable be installed on such devices.
- Pupils and Parents will be provided with a copy of these rules.

Senior School - Pupil use of mobile devices, including iPads.

1. All devices must be registered on the RGS Mobile Device Management System.
2. Pupils may not use/interfere with another pupils iPad without explicit permission.
3. Pupils must ensure their iPad is in a case.
4. iPads must not be used to make audio or video recordings or take photographic images during the school day unless permission is given by a member of staff as well as any pupil being recorded. The consent must be explicit, not implied.
5. iPads should not be used when walking around the school site, nor headphones worn.
6. iPads should not be used in school to access any form of social media like Facebook.
7. Playing games on an iPad during the school day is not permitted.
8. Pupils are responsible for ensuring there is no inappropriate material, images or video on their iPads.
9. Attempting to circumnavigate the school IT security systems is prohibited.
10. Pupils are reminded that the use of iPads is intended to enhance their learning experience, hence usage should always be appropriate to that aim. Messaging in class is therefore deemed inappropriate.
11. Pupils are reminded to store their iPad securely in their locker when not in use.
12. Pupils should store/archive their school work in the RGS provided Google Drive account.

Pupils are reminded of the importance of bringing their iPad to school, fully charged each day.
Please note this policy covers the use of both tablets and phones, regardless of manufacturer, or operating system.

Pupils are reminded of the importance of bringing their iPad to school, fully charged each day. Pupils are not permitted to bring their own cables, batteries or chargers into school unless they have bee PAT tested by the RGS Maintenance Department.

Please note this policy covers the use of both tablets and phones, regardless of manufacturer, or operating system.

Version History

Sponsor: Mr John Jones, Assistant Head, Director of Innovation
Original version 24 May 1999; Reviewed May 2000, May 2001; April 2002; March 2003, October 2004; May 2005; March 2006; June 2007; August 2008; April 2009; September 2010; May 2011; April 2012; January 2013; August 2013; June 2014; September 2014; October 2014; September 2014; October 2013; October 2015; November 2015; December 2016; May 2017; August 2017; October 2017; August 2018; August 2019, August 2020, August 2022, August 2023 and August 2024