DIGITAL SAFETY POLICY
(INCLUDING REMOTE LEARNING)

School update	
Responsible for review of policy	Assistant Head/Deputy Head Academic/Deputy Head Pastoral
Last school update	January 2022
Governor Sub-Committee approval	
Sub Committee to review and approve	Academic
Review Period	Annual
Last Sub- Committee review date	March 2022
Scheduled review	March 2023
Approved by Sub Committee (Meeting date)	9 March 2022
Version number	5
Next Sub-Committee Review	March 2023
Related policies	Safeguarding Behaviour Preventing Extremism Cyber bullying Consensual and Non-Conscience Sharing of Nudes/Semi-Nudes

Uploaded to Staff Shared	March 2022
Uploaded to Website	March 2022

Contents

1. Introduction

The Royal Masonic School for Girls (RMS) recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils, staff and governors will be able to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

This policy is designed to promote the safer use of the internet and electronic devices by all school users. In this policy the importance of technology in young people's lives is recognised and our obligation to teach them the resilience and skills required to use it well and wisely *"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim." Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review".*

This communication revolution gives young people unrivalled opportunities but it also brings risks. RMS teaches pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking, sexting and abuse. They also learn how to avoid the risk of exposing themselves to subsequent embarrassment.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

2. Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored.

CPOMS and all breaches of this policy are reported on and dealt with by the school's behaviour and/or safeguarding policy as appropriate. All breaches of this policy that may have put a child at risk must be reported to the Designated Safeguarding Lead, DSL, Ms Alison Davies.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using RMS's facilities

The School provides the I.T and communication systems for the purposes of school-related work and the use of these systems at all times is subject to this policy. Any breach of this policy will be subject to the School's disciplinary procedures and will be dealt with accordingly.

RMS also works with partners and other providers to ensure that pupils who receive part of their

education off site or who are on a school trip or residential are safe online.

RMS provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: *safeguarding, Data Protection Policy, Appropriate Privacy Policy, health and safety, behaviour, anti-bullying and cyber-bullying and ICT use of mobile technology by boarders*

4. Policy and procedure

RMS seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

RMS expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to RMS.

The use of electronic devices within schools gives particular need for caution. Specifically, the use of such means of communication between staff members and pupils must be handled sensibly and with due care and attention.

- Users should approach online communications exactly as they treat face-to-face chats, letters or telephone calls.
- A member of staff who publishes dubious or reckless material on the internet must accept the consequences if it becomes fully public. If it undermines trust and confidence between employer and employee, disciplinary action may be taken. Staff need to realise that a relationship is a relationship regardless of whether it is face-to-face or online.
- Sharing inappropriate jokes or pictures is no different from passing them around the classroom and the School would be entitled to take the view that this constitutes misconduct. Any suggestion that the sharing of material was designed to 'groom' a young person, or might be interpreted that way, would potentially be gross misconduct and might lead to dismissal.

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents/carers, and pupils and parents/carers should not attempt to discover or contact the personal email addresses or social media accounts of staff.

<u>Use of email</u>

Staff and governors must use a school email account for all official communication to ensure everyone is protected through the traceability of communication and to minimise risks of data protection

regulatory breaches. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the School system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. *For advice on emailing, sharing personal or confidential information or the need to gain parent permission* contact RMSCompliance@rmsforgirls.com. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under a subject access request

Staff, governors and pupils should not open emails or attachments from suspect sources; delete them and report their receipt to IT Support.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (e.g. cyberbullying).

Use of Social media

Use of social media can enrich what happens in the classroom; it can allow teachers to share ideas and resources to support learning. It also has many pitfalls and this policy aims to help staff use social media sites with confidence. This advice does not give prior permission to use these sites but is listed to help inform staff about some of the measures used to protect staff and students. Use of social networking applications in work time for personal use only is not permitted.

Staff who use social networking sites must check their privacy and security settings carefully and be aware if they invite people to their site or send information out this can reach a very wide audience. The Teachers' Standards make it clear that teachers are expected to demonstrate consistently high standards of personal and professional conduct.

Staff must not have any current pupil of this school added to their personal page and are advised not to include former pupils. No member of staff should communicate with current pupils via social networking sites for private purposes and should not have current pupils as "friends" or follow current pupils on other social media. Contact with former pupils should remain professional and supportive but never become familiar.

Use of social networking applications by staff do not need to be approved but:

- must not breach the School's misconduct or equal opportunities policies
- must not be used to discuss or advise any matters relating to School matters, staff, pupils or parents
- employees should not identify themselves as a representative of the School
- references should not be made to any staff member, pupil, parent or school activity/event unless prior permission has been obtained and agreed with the Head
- staff should be aware that if their out-of-work activity causes potential embarrassment for the School or detrimentally affects the School's reputation, then the School is entitled to take disciplinary action. A negative comment about the School, the staff, or pupils in the public domain is a serious breach of professional standards such actions on social media are clearly in the public domain
- staff must not provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School
- when a member of staff's employment with the School ends, for whatever reason, any personal profiles on social networking sites should be immediately amended to reflect the fact that the member of staff is no longer employed by the School.

Staff should not engage with any direct messaging of pupils through social media. Any information should be shared through a recognised school account and the message must be public.

Any incident of cyber bullying or breach in safeguarding rules must be reported immediately to the safeguarding team in line with safeguarding policy.

Staff should take extreme care to ensure that pupils are not exposed, through any medium, to inappropriate or indecent images. This includes the showing of films that are not age appropriate.

Visiting online sites and downloading

- Staff should preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Compliance Officer with details of the site/service. All users must observe copyright of materials from electronic sources.
- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.
- When working with pupils searching for images should be done through Google Safe Search (standard through our system), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, radicalisation, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring RMS or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given.
- Use RMS's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the School

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police and /or other external agencies.

RMS recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Deputy Head Academic.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of RMS. Please *refer to the appropriate Privacy Policy and the 'Policy on Taking and Using Images of Children* Photographs and images of pupils are only stored on RMS's agreed secure networks which include some cloud based services. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow RMS's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of RMS community, other than their own child/ren.

Staff and other professionals working with pupils, should only use school equipment to record images of pupils whether on or off site.

Use of personal mobile devices (including phones)

The School provides staff with mobile phones with which pupils can communicate with them for trips and out of school activities. Only in exceptional circumstances does RMS allow a member of staff to contact a pupil or parent/carer using their personal device which must be reported to the DSL.

If a pupil has sent an inappropriate text or voice message to a member of staff, it should be shown or heard by another adult at the earliest opportunity; an inappropriate call should be terminated as quickly as possible. Such incidents should be reported ASAP to the DSL or safeguarding team.

A member of staff should not instigate mobile telephone communication with a pupil, apart from in an emergency. If such communication is necessary, it is recommended that this is done while another member of staff is present.

Members of staff should not to take, store, transfer or otherwise share any images of pupils on a phone capable of taking digital images (see RMS Staff Code of Conduct)

Parents/carers may not take images at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission.

Senior School

For pupils in Years 7-11, mobile phones should be switched off and stored in the pupil's lockable classroom locker first thing in the morning and kept there throughout RMS day. Boarders' in Harris House phones should be left in their House. Phones shall not be used within the school buildings except in the Resource Centre after 4 pm only, where they may be *monitored* with respect to pickups and meetings. *Monitored* means the phone may be on the desk on silent/vibrate; if a call/text needs to be made the student should go outside the RC.

If a pupil in Years 7-11 is found with a mobile phone during RMS day, it will be confiscated and stored in Reception, New Mark Hall.

Reception informs parents by email that the phone has been confiscated and will be kept overnight and until 4pm the following day. The pupil may collect the phone from Reception at 4pm at the end of the day **after** the overnight confiscation period. Phones confiscated on a Friday may be collected at 4pm on the following Monday.
If a pupil repeatedly contravenes these rules, further sanctions will be imposed.

Sixth Form

Sixth Formers are permitted to use personal electronic devices in their Common Room and in lessons only with teacher permission.

Mobile phones should not be used or visible around school except in the Resource Centre after 4pm where they may be *monitored* with respect to pickups and meetings. *Monitored* means the phone may be on the desk on silent/vibrate; if a call/text needs to be made the student should go outside the RC.

If a Sixth Former uses a personal electronic device inappropriately, it will be confiscated and the same procedure will apply as detailed above

Cadogan House

No pupil in Cadogan House, day or boarder is allowed to bring a mobile phone to school without written permission from the Head of Cadogan House. This permission is usually confined to those pupils using RMS coaches although it may be granted in other, exceptional circumstances. If permission has been granted then the phone should be handed into the Cadogan House office at the beginning of the day and collected immediately prior to leaving to catch the coach.

If a pupil in Cadogan House is found with a mobile phone during RMS day, it will be confiscated and stored in the Cadogan House office.

The confiscated electronic device must be collected by the pupil's parent. It will not be returned to the pupil directly. The pupil herself must notify her parents/guardians of the confiscation.

If a pupil repeatedly contravenes these rules, further sanctions will be imposed.

Under no circumstance should pupils use their personal mobile devices/phones to take images of
- any other pupil unless they and their parents have given agreement in advance
- any member of staff

RMS is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

<u>New technological devices</u>

New personal technological devices may offer opportunities for teaching and learning. However, RMS must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with Assistant Headteacher before they are brought into school.

<u>Reporting incidents, abuse and inappropriate material</u>

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the safeguarding team, the Headteacher. Where such an incident may lead to significant harm, safeguarding procedures must be followed. RMS takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police, as per the safeguarding policy.

Systems and Access

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

- Computer storage areas are school property.
- Sensitive data or contact details must not be copied from the school database
- All emails (even when deleted) and their history are logged.
- Members of the IT staff may look at any files and communications to insure that the system is being used responsibly
- Particular care must be taken when using iPads to follow the School's safeguarding and IT policies.
- The School filters access to inappropriate sites with filtering technology used to provide a safe platform within the school system.

Vulnerability to radicalisation or extreme view points

The School recognises its duty to protect our students from indoctrination into any form of extreme ideology which may lead to the harm of self or others. This is particularly important because of the access to electronic information through the internet. The School safeguards young people through educating them on the appropriate use of social media and the dangers of downloading and sharing inappropriate material which is illegal under the Counter-Terrorism Act together with filtering technology to provide a safe platform.

Additional Information

- All users are required to log on to the School network with their own personal username, which will remain with them throughout their time at the School.
- All users have their own password to allow them to log on, which should not be made available to anyone else.
- Do not reveal your password to anyone. If you think someone has learned your password then change it immediately. Use a minimum of eight characters. Do not write your password down
- Remember a school is a public place. Always make sure that you have completely logged off the computer before leaving it unattended. Failure to do so will be considered a contravention of school policy and if an offence has been committed by some other person, may be considered as facilitating the Misuse of Computer, which is also a criminal offence
- Use of another person's username and password is considered a criminal offence under the Computer Misuse Act 1990 and/or depending on offence any other Act listed below.
- You should not trespass in others' folders, work or files. All unauthorised access is considered a criminal offence under the Computer Misuse Act 1990 and/or depending on offence any other Act listed below.
- Damage to data, computers, computer systems or computer networks, including unauthorised damage or interference to any files or program is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.
- Programs must not be installed on a computer except by a member of the IT administration department.
- The unauthorised copying of software, contrary to the provisions of the Copyright, Designs & Patents Act 1988, is not permitted.

File Security

- All users have their own area for storing their work on the network server. This means that they can access their work from any network station and indeed from home; see later.
- Users are not permitted access to station and network drives other than those provided at login nor are they permitted to alter or save files outside their own area (except in the authorized shared areas).

The following are not permitted:

- Use of another person's username and password.
- Trespass in others' folders, work or files.
- Hacking or attempted hacking with intent to cause damage.
- Moving or changing any computer or associated equipment unless specifically requested and authorised by a member of IT staff. Damage caused by unauthorised persons may be considered a criminal offence.
- Undertaking financial transactions on behalf of the school unless authorised.

Access to Software

- All users receive desktop icons and start-menu-shortcuts to all the main application programs and common utilities.
- Users are guided onto the network via shortcuts. This provides shortcuts/icons to programs that are relevant as well as any shared documents provided by the subject teachers. Students have read-only access to these shared documents but may copy them for their own use. Attempts to modify these are in breach of the Computer Misuse Act
- Users can only access software and other resources as made available to them through these shortcuts. For example, students do not have access to the Staff areas.

Access to Printers

You are encouraged to manage printing sensibly. Only print when a hard copy is necessary.

Use of personal devices or accounts and working remotely

When working remotely do not use open or shared Wi-Fi and always use your school email address, not a personal one. If you download personal data, ensure that your home machine/device is adequately security protected with passwords and security updates and always delete files which are no longer needed, including from your 'downloads' folder and your 'recycle bin'; do not save access passwords to personal devices. If you carry documents containing personal data home, never leave them in your car and keep them in a secure location where no one else will have access. Never store personal data on a USB stick.

5. Curriculum

Online safety is embedded within our curriculum. RMS provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)
- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

6. Staff and Governor Training

As part of their safeguarding training, staff and governors are trained to fulfil their roles in online safety. RMS audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

Staff are provided with a copy of the online safety policy and must sign RMS's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Guidance is provided for all members of the school community in this policy.

7. Working in Partnership with Parents/Carers

RMS works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. During lessons, teachers will guide students toward appropriate materials. Outside of lessons, families and/or parents/carers bear responsibility for such guidance, as they do with other information sources such as television, telephone, cinema, radio, newspaper, magazine and other potentially offensive media. RMS seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. RMS provides regular updated online safety information through the RMS website and by other means.

Parents/carers are asked, at the change of Key stage or following a significant update, to discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix F. The Acceptable Use Agreement explains RMS's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

8. Records, monitoring and review

RMS recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged in CPOMS. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

RMS supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under RMS's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

Response to Misuse

Any breach of these policies and protocols will be dealt with using the school's disciplinary procedures.

Sanctions will be in line with our behaviour management policies and will include, but not be restricted to; detentions, formal warnings, re-education and in some cases exclusions.

Where applicable police and/or local authorities may be involved.

Illegal activity will always be reported to the police and/or Hertfordshire Safeguarding Children Partnership.

Statutory guidance for dealing with electronic devices

- Students should be aware that staff have the right to ask to examine their digital device. If a breach

of the behaviour code is suspected, an **electronic device** may be examined and any data or files on the device may be searched if they think there is a good reason to do so.

- The member of staff must have regard to the following guidance issued by the Secretary of State when determining what is a "good reason" for examining or erasing the contents of **an electronic device:**
  In determining a 'good reason' to examine or erase the data or files the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules
- The School reserves the right to seek advice from external bodies eg. police/CPSLO to support a proportional response which follows best practice.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes.

9. Appendices of the Online Safety Policy

A. Online Safety Guidance for Any Staff* and Governors
B. Acceptable Use Policy for pupils - Senior School
C. Online Safety Guidance for Cadogan House
D. Online safety policy guidance - Summary of key parent/carer responsibilities
E. Guidance on the process for responding to cyberbullying incidents
F. Guidance for staff on preventing and responding to negative comments on social media
G. Online safety incident reporting form / Evidence for CPOMS
H. Student IPAD/Laptop/Tablet Acceptable Use
I. Agreement for Loan of iPad or Chromebooks to RMS Staff
J. RMS Wi-Fi Guidance

Appendix A - Online Safety Guidance for Any Staff* and Governors
***including student teachers who are members of staff, visiting music teachers, coaches and volunteers**

You must read this agreement in conjunction with the online safety policy and the Staff Privacy Policy and Data Protection Policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in RMS. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Assistant Headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring RMS, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the Assistant Headteacher.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. Contact with former pupils will remain professional and supportive but never become familiar.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage RMS, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to RMS or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared. I will not save access passwords to personal devices.

Data protection

I will follow all requirements for data protection explained to me by RMS. These include:

- I understand that there are strict controls and requirements regarding the taking and use of images. I will follow all the requirements in the *POLICY ON TAKING AND USING IMAGES OF CHILDREN* and the *school code of conduct*.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements on the Data Protection Policy and Privacy Policies.

Use of personal devices or accounts and working remotely

When working remotely I will not use open or shared Wi-Fi. My home machine/device is adequately security protected with passwords and security updates if I need to download personal data. I will always delete files which are no longer needed, including from my 'downloads' folder and my 'recycle bin'. If I carry documents containing personal data home they will be kept safely and securely. Personal data will not be stored on a USB stick.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where permission has been granted and as per guidance of the Data Protection Policy and Privacy Policies.

School devices should be used to take images, sound recordings or videos of tuition or wider school activities. If personal devices have to be used the image must be uploaded and deleted.

Use of email

I will use my school email address for all school business. All such correspondence must be kept professional and is open to Subject Access Requests. I will not use my school email addresses for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Network manager.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL or DDSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the Deputy Head Academic.

Appendix B - Acceptable Use for pupils - Senior School

Acceptable Use Policy Remote Learning Senior School form

ALL PUPILS ARE EXPECTED TO ADHERE TO THE GUIDANCE AND RULES CONTAINED WITHIN THIS DOCUMENT

1/14/22, 10:52 AM Acceptable Use Policy Remote Learning Senior School form

1. Online Safety Acceptable Use Agreement – Senior School

Tick all that apply.

- [ ] I will use school IT equipment for school purposes only.
- [ ] I will not download or install software on school IT equipment.
- [ ] I will only log on to RMS network, other school systems and resources using my own school user name and password.
- [ ] I will not reveal my passwords to anyone.
- [ ] I will not use my personal email address or other personal accounts on school IT equipment or to communicate with staff.
- [ ] I will make sure that all my electronic communications are responsible and sensible.
- [ ] I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- [ ] I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff if I am in school, or parent/carer if I am not in school.
- [ ] I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will report immediately any request for personal information, to a member of staff if I am in school or parent/carer if I am not in school.
- [ ] I should never post photographs, videos or livestream without the permission of all parties involved.
- [ ] I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of RMS community.
- [ ] I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in RMS community or bring RMS into disrepute.
- [ ] I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- [ ] I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.
- [ ] I will not attempt to bypass the internet filtering system in school.
- [ ] I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.
- [ ] I will not lie about my age in order to sign up for age inappropriate games, apps or social networks.
- [ ] I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- [ ] I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

- [ ] I will follow the guidance set out in the Appendices in this policy.

2. Rules

Tick all that apply.

- [ ] I will only use technology for school purposes as directed by my teacher.
- [ ] I will only use Google Meet when directed by the teacher.
- [ ] I will not record or take photos of my classmates or teachers during a Google Meet session.
- [ ] I will not reveal my passwords to anyone.
- [ ] I will be responsible for my behaviour and actions when using technology (Google Meet and other interactive applications), this includes the resources I access and the language I use.
- [ ] I will make sure that all my communication with students, teachers or others using technology is responsible and sensible. If sending email I will only use my school email account.
- [ ] I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher or my parent.
- [ ] I understand that when using Google Classroom and other applications provided by the school that my use can be monitored and logged and can be made available to my teachers.
- [ ] I understand that these rules are designed to help keep me safe and that if they are not followed, school sanctions will be applied and my parent may be contacted.

3. Guidelines When using Google Classroom, remember that this is an extension of the classroom and you should conduct yourself as you would in a classroom. This includes:

Tick all that apply.

- [ ] Video conferencing from an environment that is quiet, safe and free from distractions (not a bedroom)
- [ ] Be on time for your interactive session
- [ ] Be dressed appropriately for learning (i.e. no pyjamas)
- [ ] Remain attentive during sessions
- [ ] Interact patiently and respectfully with your teachers and peers
- [ ] You MUST NOT record each other's online interactions.
- [ ] Make sure you end the session as soon as the teacher indicates to do so.

Netiquette For Remote Learning

4. Lessons

Tick all that apply.

- [ ] You should be in a common area in the house with good wifi, not your bedroom, where your parents can monitor your work
- [ ] You should have all the equipment you need for that lesson ready for the start of the lesson as usual
- [ ] Normal rules of the classroom apply with regards to your behaviour and completion of work
- [ ] Assignments/Homework should be done to the best of your ability and submitted on time
- [ ] If you are unsure of a task or need assistance use Google Stream (within classroom) to ask a question. If you get behind on your work, please let your class teacher know so that they can help you.

5. Google Meets

Tick all that apply.

- [ ] When using Google Meet you should be appropriately dressed, your electronic device should be stable and facing you and you should not wander around with it during the lesson.
- [ ] You should be mindful that you are visible at all times as is your background which is being shared with the class - it is easy to forget!
- [ ] Microphones should be muted unless you have been asked to speak. One to one meetings on Google Meet with teachers are not the norm. If this takes place then the meeting will be recorded.
- [ ] You are not permitted to film or record the lessons. Make sure you end the session as soon as the teacher indicates to do so.
- [ ] The School rules and Acceptable Use Policy apply to all remote learning – poor online behaviour will be dealt with robustly by staff using the School's sanctions system and there will be follow-up contact with your parents.

Appendix C - Online Safety Guidance for Cadogan House

My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of RMS community.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with Mr Connors.

Please return the signed sections of this form which will be kept on record at RMS.

Pupil agreement

Pupil name……

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature……..

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring RMS or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about RMS would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of RMS, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of RMS unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……

Parent/carer signature……..

Date ……..…

Appendix D - Online safety policy guidance - Summary of key parent/carer responsibilities

RMS provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check RMS policy.
- All cyberbullying incidents affecting children in RMS should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) RMS will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable, block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- RMS may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses RMS name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring RMS or any individual within it into disrepute. Negative postings about RMS would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of RMS, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on RMS website.

Appendix E - **Guidance on the process for responding to cyberbullying incidents**

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of RMS community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix F - **Guidance for staff on preventing and responding to negative comments on social media**

If used correctly, parents can use a school's social media's site as a source of reliable information. The online safety policy, see especially Appendix F (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using RMS's name or logo.

RMS should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring RMS into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with RMS should be used.

If negative comments are posted:

- Collect the facts which may involve screenshots.

As soon as you become aware of adverse comments relating to RMS you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow RMS's safeguarding procedures.

If there is a risk of serious damage to RMS reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of RMS community.

- Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that RMS will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix G - Online safety incident reporting form / Evidence for CPOMS

Any member of RMS community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below or use it for guidance to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this

report to the DSL. Alternatively use this form for inputting information on CPOMS.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or RMS into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?

Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Immediate action taken following the reported incident including dates:	
Incident reported to online safety Coordinator/DSL/ DSP/Headteacher	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix H Student IPAD/Laptop/Tablet Acceptable Use

At RMS we are building on our successes in the classroom by incorporating mobile technology. We are enhancing our traditional teaching to create a modern learning environment which will continue to encourage the four Cs:

Creativity
Critical Thinking
Collaboration

Challenge

Ready access to tablet devices will ensure our students are afforded the opportunities that technology presents to young learners and their learning. Technology will be the servant not the master.

What this Agreement covers

This laptop/tablet Acceptable Use Home/School Agreement relates to:
(1) any use of RMS owned laptops/tablets in School
(2) personal laptops/tablets used in School and
(3) All laptops/tablets used for School purposes irrespective of ownership.

It does not relate to the use of laptop/tablets by Boarders out of School hours which is regarded as similar to home use and covered by the Use of Mobile Technology for Boarders Agreement

The purpose of this Agreement

This agreement is to promote responsible use and protect students and RMS from any misuse of the laptop/tablet. We want the laptop/tablet to become a useful tool for learning and for setting challenging and engaging learning experiences. We are aware of the risks associated with using new technology in this way and we have tried to provide detailed guidelines on how we will work, with your help, to manage these risks as much as possible. All laptop/tablets to which this Agreement relates must be used in accordance with RMS's Online safety policy and other acceptable use documents. Teachers may set additional requirements for use in their respective classes. The policies governing the use of the laptop/tablet support its academic use.

What RMS requires from you

To maintain the integrity of the laptop/tablet programme, all students and parents/guardians must acknowledge and agree to the following conditions of use:

A. General Principles

Remember that access to devices and the Internet is a privilege, not a right and that access requires responsibility.

RMS needs to ensure that users are using the system responsibly. Consequently, users should not expect that stored files will always be private. Staff members have the right to look at the content stored on any laptop/tablet to which this Agreement relates at any time and they may review files and communications. In the normal course of laptop/tablet usage, it is unlikely to be necessary to invoke this power, but it is there to prevent any mis-use of the iPad or using the iPad during a lesson for any purpose other than stated by the teacher. More in depth investigations will follow the guidance in the digital safety policy.

Unfortunately, as well as containing some incredible resources to support students' learning, the Internet comes with dangers. You must report anything that you feel uncomfortable about, or that you think is inappropriate, to an appropriate member of staff (in line with ICT Network Agreement) or, if out of school, parents/guardians and if applicable the police via CEOP. Further information can be found at http://www.thinkuknow.co.uk/11_16/

B. Laptop/tablet Ownership and Care

1. Each student may to bring to School a laptop or tablet device.
2. Students are responsible for knowing how to properly operate and protect the laptop/tablet. This includes not leaving the laptop/tablet in a location where it can be damaged or stolen.
3. Students/Parents are solely responsible for the care and security of student laptops/tablets. Laptops/tablets must never be left in an unlocked locker or any unsupervised area. The laptop/tablet must be kept in its protective case at all times.
4. It is strongly recommended that parents avail themselves of insurance cover for the laptops/tablets.

5. If the laptop/tablet is lost or stolen, the student must report the incident as soon as possible.
6. When travelling to and from and around School laptops/tablets should be kept out of sight.

C. General Expectations

1. Students must use the devices in accordance with the ICT Network Use Agreement.
2. Students may install School software, including Lightspeed MDM.
3. While in School, students may only connect to the Internet via the wireless network provided by the RMS.
4. Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
5. Laptops/tablets must bear the student's name.
6. The use of the laptop/tablet in School is always at the teacher's discretion:
   The laptop/tablet may only be used with the permission of the member of staff.
   The laptop/tablet may only be used for the purpose expressed by the member of staff.
7. Any use of the laptop/tablet for playing games will result in significant sanctions.
8. There must be no recording (video, photographs or audio) unless the permission of the member of staff has first been obtained and then only subject to any conditions imposed.
9. All recorded material is for your personal use only and must not be placed in the public domain (e.g. Facebook, YouTube etc.).
10. Recording another pupil or a member of staff without their permission will be treated extremely seriously. Permission must always be sought and obtained first.

D. Use at School outside lessons

We want to encourage students to work collaboratively with their laptop/tablet in their own time, however it is essential that students spend time away from the device and take a break.

1. Year 11 students will only be allowed to use their laptops/tablets during break and lunchtimes in already established IT areas. The Sixth Form may also use them in their Study and Common Rooms.
2. The laptop/tablet must only be used in School for matters related to the student's own lessons.
3. The laptop/tablet must not be used in School for playing games, using social networks, entertainment (e.g. watching a video on YouTube unrelated to your studies) or communication except by email or one of the pre-loaded apps.
4. All email use must be using the account allocated by the School.

E. Apps, Files, Etc.

1. Students are expected to back up all educational work from the laptop/tablet.
2. During the School day, permission may be given for use of earphones in a classroom by a teacher.
3. When using the laptop/tablet camera, students may not distribute, publish, post, email or share images and/or videos of students or staff beyond the scope of the learning task.

F. The following are prohibited:

1. Leaving the laptop/tablet unattended in School.
2. Exchanging laptops/tablets with another student.
3. Allowing other students to retain or remove the laptop/tablet from their presence.
4. Copying certain Internet materials or reproducing or transmitting materials without the permission of the author or other right-holder.
5. Plagiarising academic materials. It is the student's responsibility to respect and adhere to all copyright, trademark and other intellectual rights and trade secrets laws.
6. Using the laptop/tablet for any action that violates existing School rules or public law.
7. Creating, accessing or distributing offensive, bullying/threatening, obscene, rumours/gossip, sexually explicit or other content as outlined in the RMS Network Acceptable Use Agreement.
8. Use of chat rooms or messaging services not authorized by the teacher for academic use.
9. Accessing sites selling book reports, and other forms of student work.

10. Spamming: sending mass or inappropriate emails.
11. Gaining access to other students' accounts, files, and/or data.
12. Use of the School's internet/E-mail accounts for financial or commercial gain outside of school sanctioned projects such as Young Enterprise or for any illegal activity.
13. Sharing passwords, addresses, or other personal information on the Internet.
14. Using or possessing hacking software.

Appendix I Agreement for Loan of iPad or Chromebooks to RMS Staff

Name:

Department:

Device Number:……Machine serial number:

I acknowledge receipt of the above device in good working order, with charger, cable and case.

I understand and agree that:

1. The device is allocated to me for my professional use in connection with teaching at the School.

2. I understand and agree that any personal use must be small, as anything other may give rise to a potential tax liability for me.

3. I acknowledge that the security of the device is my responsibility. If the device is taken home by car it must be locked in the car and out of sight. It must not be left unattended at any time, and if left at home must be stored in a safe place.

4. The device must be promptly returned to the School on request of the Head Teacher or Bursar and in any event on the last school day before leaving the School's employment. It may be charged in any location, but must be returned to the IT Department on request for updates or synchronisation.

5. Any photographs or videos taken of students on the device must be for School use only. No personal or students' personal data, files or images may be stored on the iPad.

6. Particular care must be taken when using the device to follow the School's safeguarding and IT policies. The School will randomly check devices and check through search histories to verify policies are being followed. Action will be taken where necessary and the appropriate authorities will be informed in line with safeguarding procedures.

7. I understand the need to keep information secure and the consequences of not doing so. I will protect access to the device with an alpha-numeric password and where possible, password protect applications and websites with different passwords.

8. Any damage to the device will be the responsibility of the user. Although insurance is held by the School to cover accidental damage, if such damage is deemed to be due to my negligence I may be liable for any insurance excess payable.

Signed: Date

Appendix J RMS Wi-Fi Guidance

As a professional organisation with responsibility for children's safeguarding it is important that all members of the School community are fully aware of the School's boundaries and requirements when using the School Wi-Fi systems. All possible and necessary measures should be taken to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the School community are reminded that ICT use should be consistent with the School ethos, other appropriate policies and the Law.

Please be aware that the School will not be liable for any damages or claims of any kind arising from the use of the WiFi service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

The School provides Wi-Fi for the School community and allows access for education, research and revision. Access to the WI-FI network is available throughout the main building of the School. Users will need to logon using their School username and password.

In the case of visitors to the School requiring Wi-Fi access a Guest username and password will be generated for that visit by the IT Team. This will be a 'one-off' password and will be deleted once the visitor no longer requires it.

You are asked to sign below to indicate your understanding and agreement to the following:

1. I agree to comply with the School's Acceptable Use Policy, e-Safety policy and behaviour policy in respect of the use of ICT devices

2. I understand that the School reserves the right to limit the bandwidth of the WiFi service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. School-owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. *nb. Computer material includes but are not limited to programs, Databases, and files not relevant to the user.*

4. I will take all practical steps necessary to make sure that any equipment connected to the Schools service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. The School's wireless service is not secure, and the School cannot guarantee the safety of traffic across it. Use of the School's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the School harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

6. The School accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the School's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the School from any such damage.

7. The School accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the School's wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information

system unattended without first logging out or locking my login as appropriate.

9. I will not attempt to bypass any of the School's security and filtering systems or download any unauthorised software or applications.

10. My use of the School Wi-Fi will be safe and responsible and will always be in accordance with the School AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the School into disrepute.

12. I will report any e-Safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead Ms Alison Davies, The Safeguarding team and/or the Network Manager Mr P Elder as soon as possible and as appropriate.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Mr D Cox, Assistant Head.

14. I understand that my use of the School's internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the School suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the School will terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes then the matter may be brought to the attention of the relevant law enforcement organisation.