The Rudheath Senior Academy

E-safety Policy

Document Detail	
Reference Number	RSA030
Category	School
Author	Deputy Head Teacher: Safeguarding
Issue Date	September 2021
Last Review Date	September 2024
Next Review Date	September 2025

1. INTRODUCTION

1.1 The Rudheath Senior Academy (RSA) recognises that ICT and the internet are tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence.

1.2 Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice responsible e-safety.

1.3 It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online. The importance of this has been highlighted through the recent period where students and staff are having to work remotely.

1.4 E-safety covers the internet, mobile phones and other electronic communications technologies. Some adults and young people may use these technologies to harm children.

1.5 The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

1.6 There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.

1.7 Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through behaviour and anti-bullying procedures of the school which are outlined in the relevant school policies.

2. AIMS

2.1 This policy aims to be an aid in regulating ICT activity in school, and provide a robust understanding of appropriate ICT use that members of the school community can use as a reference for their conduct when outside of RSA. E-safety is a whole-school issue and responsibility.

2.2 This policy also aims to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. Additionally, the school will provide the necessary safeguards to help to ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

2.3 This policy applies to all members of The Rudheath Senior Academy (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of The Rudheath Senior Academy ICT systems, both in and out of the school.

2.4 The Education and Inspections Act (2006) empowers Principals and Head Teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

2.5 The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the school.

2.6 All users are required to read and accept this E-Safety Policy when first accessing RSA's systems and all students must agree to and sign the Acceptable Use of ICT and Communications Systems Agreement set out at Appendix A annually.

3. ROLES AND RESPONSIBILITIES

3.1 The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

3.1.1 **Local Governing Body:**

3.1.1.1 The Local Governing Body are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body and North West Academies Trust will be appointed as a link for Safeguarding.

3.1.2 **Senior Leadership Team (SLT):**

3.1.2.1 The SLT are responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety.

3.1.2.2 The SLT are responsible for ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

3.1.2.3 The SLT will ensure that there is a system in place to allow for monitoring and support of those in the school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

3.1.2.4 The SLT will receive regular monitoring reports from the ICT Officer.

3.1.2.5 The SLT should be aware of the procedures to be followed in the event of a serious e- safety allegation being made against a

member of staff. These procedures are explained in the RSA safeguarding policy.

3.1.3 **Deputy Head Teacher (Safeguarding):**

3.1.3.1 Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.

3.1.3.2 Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

3.1.3.3 Provides training and advice for staff.

3.1.3.4 Liaises with ICT technical staff including sponsors and IT support contractors.

3.1.3.5 Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

3.1.3.6 Meets regularly with the Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs.

3.1.3.7 Attends relevant meetings of Governors.

3.1.3.8 Reports regularly to SLT.

3.1.4 **IT Managed Service (Universal Technologies Ltd):** The IT services provider is responsible for ensuring:

3.1.4.1 That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

3.1.4.2 That the school meets the e-safety technical requirements outlined in this policy and any relevant e-safety policy and guidance.

3.1.4.3 That users may only access the school's networks through a properly enforced.

3.1.4.4 Password protection policy, in which passwords are regularly changed.

3.1.4.5 The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

3.1.4.6 That he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

3.1.4.7 That the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be

reported to the Pastoral Team and reported on to the relevant reporting level as described in section 5.11 below.

3.1.4.8 That monitoring software/systems are implemented and updated as agreed in school policies.

3.1.4.9 Implements software which alerts Safeguarding staff to any potential risks to students, as well as any inappropriate activity.

3.1.4.10 Supports with remote learning through the use of Office 365 and other relevant application.

3.1.5 **Teachers and Support Staff:** All staff are responsible for ensuring that:

3.1.5.1 They have an up to date awareness of e-safety matters and of the school e-safety policy and practices.

3.1.5.2 They have read and understood the staff acceptable use of ICT policy.

3.1.5.3 They monitor the activity of their students on the Virtual Learning Environment (VLE) on the courses to which they act as teachers, tutors or administrators and.

3.1.5.4 They report any suspected misuse or problem to the relevant person for investigation/action/sanction.

3.1.5.5 Digital communications with students are on a professional level and only carried out using official school systems.

3.1.5.6 E-safety issues are embedded in all aspects of the curriculum and other school activities.

3.1.5.7 Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.1.5.8 They monitor ICT activity in lessons, extra-curricular and extended school activities, including the use of teams.

3.1.5.9 They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

3.1.5.10 In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.1.6 **Designated Safeguarding Lead (DSL):** The DSL Should be trained in e-safety issues and be aware of the potential for serious student protection issues to arise from:

3.1.6.1 Sharing of personal data.

3.1.6.2 Access to illegal/inappropriate materials.

3.1.6.3 Inappropriate on-line contact with adults/stranger.

3.1.6.4 Potential or actual incidents of grooming.

3.1.6.5 Cyber-bullying.

3.1.7 **Students:** All students are to be trained during induction and as part of their PSHE programmes so that they are responsible for:

3.1.7.1 Using the school's ICT systems in accordance with the Acceptable Use of ICT and Communications Systems Agreement , which students will be required to sign upon induction to RSA.

3.1.7.2 Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright.

3.1.7.3 Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

3.1.7.4 Knowing and understanding school protocols on the use of mobile phones, digital cameras and hand held devices.

3.1.7.5 Knowing and understanding school policies on the taking and use of images and on cyber-bullying.

3.1.7.6 Understanding the importance of adopting robust e-safety practice when using digital technologies out of The Rudheath Senior Academy and realise that the school's E-Safety Policy covers their actions out of the school if related to their membership of The Rudheath Senior Academy.

3.1.7.7 Using Office 365 correctly, communicating with staff a peers appropriately and reporting any misuse of the applications.

3.1.8 **Parents and Carers:** Parents/Carers play a crucial role in ensuring that students understand the need to use the internet/mobile devices in an appropriate way, especially when having to work remotely. RSA will therefore take every opportunity to help parents understand remote learning, through parents' evenings, newsletters, letters, website, information about e-safety campaigns, literature. Parents and carers will be responsible for:

3.1.8.1 Endorsing the school's Code of Conduct contained with the Acceptable Use of ICT and Communications Systems Agreement at Appendix A.

3.1.8.2 Accessing the school website in accordance with this policy.

3.1.8.3 Ensuring their child uses the school IT systems effectively whilst outside of RSA.

3.1.9 **Visitors:** Visitors who access the school's ICT systems will be expected to adhere to this policy and will be monitored accordingly. They will be informed of these policies on entry to the system.

4. POLICY STATEMENTS

4.1 Education - Students

4.1.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Students and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

4.1.2 E-Safety education is provided in the following ways:

4.1.2.1 A planned e-safety programme will be provided as part of PSHE. This should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. This will involved drop down days and visits from relevant external bodies.

4.1.2.2 Key e-safety messages should be reinforced as school displays and information posters.

4.1.2.3 Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

4.1.2.4 Students should be helped to understand the need for an E-Safety Policy and Acceptable Use of ICT and Communications Systems Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

4.1.2.5 Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. (Information available from Learning Resource Centre).

4.1.2.6 Staff should act as good role models in their use of ICT, the internet and mobile devices. Students will be informed that mobile devices

will not be used in lessons as part of (as identified in the school Behaviour Policy.

4.1.3 **Education - Parents and Carers**

4.1.3.1 Many parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of the student and in the monitoring/regulation of the student's on- line experiences.

4.1.3.2 Parents often either underestimate or do not realise how often students and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

4.1.3.3 The school will therefore seek to provide information and awareness to parents and carers through: letters, newsletters, web site, social media, parents evenings.

4.2 **Education and Training – Staff**

4.2.1 It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

4.2.1.1 Planned formal e-safety training will be made available to staff beginning with their Induction Programme covering Safeguarding and NWAT Staff Code of Conduct. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

4.2.1.2 All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Policies.

4.2.1.3 The pastoral team will receive regular updates through attendance at external training sessions and by reviewing guidance documents released by the LA and others.

4.2.1.4 This E-Safety policy and its updates will be presented to and discussed by staff in staff/ team meetings/CPD days.

4.2.1.5 The pastoral team will provide advice / guidance / training as required to individuals as required.

4.2.1.6 The designated safeguarding leads, PSHE leader and IT Officer will meet weekly to discuss ongoing issues regarding e-safety.

4.3 **Training – Governors and Trust Members**

4.3.1 Governors and Trust Members should take part in e-safety training/awareness sessions, with particular importance for the Safeguarding link(s). This may be offered in a number of ways:

4.3.1.1 Attendance at training provided by the Local Authority or other relevant organisation.

4.3.1.2 Participation in school training/information sessions for staff or parents.

4.4 **Technical – Infrastructure/Equipment, Filtering and Monitoring**

4.4.1 The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

4.4.1.1 The Rudheath Senior Academy ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in this policy.

4.4.1.2 There will be regular reviews and audits of the safety and security of school ICT systems.

4.4.1.3 Servers, wireless systems and cabling must be securely located and physical access restricted.

4.4.1.4 All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the IT Systems technician and will be reviewed annually by the governors.

4.4.1.5 All users will be provided with a username and password and users will be required to change their password every 60 days for staff and 90 days for students.

4.4.1.6 Generic log-ons will have restricted access to the internet and must be used only when students are under direct supervision by a teacher or member of staff. Generic log-ons will be used only in exceptional circumstances and will be removed at the earliest opportunity.

4.4.1.7 The “master/administrator” passwords for the school ICT system, used by the IT systems technician must also be available to the pastoral team. No person will have sole access to the IT systems.

4.4.1.8 Ssers will be made responsible for the security of their username and password and must not allow other users to access the systems

using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

4.4.1.9 The school in partnership with its stakeholders and IT systems contractors maintain and support a managed filtering service.

4.4.1.10 Any filtering issues should be reported immediately to the pastoral team.

4.4.1.11 A web filtering change log must be kept by the IT Systems Technician so that in the event of needing to switch off or change the filtering (i.e. requests from staff for sites to be removed from or added to the filtered list) the pastoral team must consider the request and if agreed they are recorded. The change log shall be reviewed regularly by the Safeguarding link(s).

4.4.1.12 The Rudheath Senior Academy ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Staff Information and Communications Systems Policy and Student Acceptable Use of ICT and Communications Systems Agreement (as applicable).

4.4.1.13 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. Proxy servers and Firewalls, Antivirus software, internet filtering and Classroom Management software are utilised throughout.

4.4.1.14 The provision of temporary access for “guests” (e.g. trainee teachers, visitors) onto the school system is in place; guest accounts will be generated with access levels agreed by line managers. These accounts will be set to automatically time out and have to be reviewed and renewed if required after an agreed time scale – a maximum 1 month.

4.4.1.15 No executable files will be downloaded by users. The IT Systems Technician will control the people allowed to download executable files.

4.4.1.16 School laptops and mobile devices are to be used for school business only. Personal use is not acceptable.

4.4.1.17 Staff can install programmes/software on their PCs/portable devices only with permission from ICT technical staff. All users accessing school devices will be restricted from downloading/installing software using a rights management application. Only IT Services will have sufficient level of rights to allow software download/installation.

4.4.1.18 The use of removable media is not permitted in RSA.

4.4.1.19 The school infrastructure and individual workstations are protected by up to date Anti-virus software. The IT Systems Technician is responsible for ensuring this software is kept up to date.

4.4.1.20 The school uses software which alerts safeguarding staff to any inappropriate/dangerous behaviour which could impact the safety of students and staff.

5. CURRICULUM

5.1 E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

5.2 In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

5.3 Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites visited.

5.4 It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation like this, staff can request that the Network/Infrastructure Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, i.e. written request (email) with clear reasons for the need and recorded.

5.5 Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;

5.6 Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

6. USE OF DIGITAL AND VIDEO IMAGES – PHOTOGRAPHIC/VIDEO

6.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet.

6.2 Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

6.3 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites staff are allowed to take digital/video images to

support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

6.4 Written permission must be sought and gained before digital images are taken and published on any externally hosted or accessible websites.

6.5 Students must not take, use, share, publish or distribute images of others without their permission.

6.6 Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

6.7 Photographs published on a website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

6.8 Students' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless authorised.

6.9 Written permission from parents/carers of young people will be obtained before photographs of these students are published on the school website or any publicity material.

6.10 Students work can only be published with the permission of the student and parents or carers of students.

7. USE OF DIGITAL AND VIDEO IMAGES – PHOTOGRAPHIC/VIDEO

7.1 Information which is recorded and retained is compliant with Data Protection and GDPR legislation. Personal data will be processed in line with the RSA Data Protection Policy which can be found on Microsoft Teams or requested from the Business Manager.

7.2 In particular, staff must ensure that they:

7.2.1 use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

8. COMMUNICATIONS

8.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages.

9. ICT GOOD PRACTICE

9.1 When using communication technologies, The Rudheath Senior Academy considers the following as good practice:

9.1.1 The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access or Microsoft Teams).

9.1.2 Users need to be aware that email communications may be monitored.

9.1.3 Users must immediately report, to the nominated person – in accordance with the sollege policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

9.1.4 Any digital communication between staff and students or parents/carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.

9.1.5 Students will be provided with individual school email addresses for educational use.

9.1.6 Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

9.1.7 Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. UNSUITABLE/INAPPROPRIATE ACTIVITIES

10.1 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would therefore be banned from school and all other ICT systems. Other activities such as cyber- bullying would also be banned.

10.2 Users should be aware that inappropriate internet activity is taken seriously and could lead to disciplinary action and/or criminal prosecution.

1. MONITORING AND REVIEW

1.1 The Head Teacher, Designated Safeguarding Lead and ICT Officer monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

Appendix A: Student Acceptable Use of IT and Communication Systems Agreement

The Rudheath Senior Academy

IT and Communications systems are integral to the lives of young people, both within education and outside of education. The Rudheath Senior Academy recognises the educational value of IT and Communications systems and acknowledges their potential to support student's learning and the curriculum. Every effort will be made to provide quality experiences for students using IT and Communications systems.

This Acceptable Use Agreement deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones, mobile telephones, tablets, personal digital assistants (PDAs) and voicemail.

Misuse of IT and communications systems can damage the business and reputation of RSA. It could also lead to serious consequences for students who use systems in an inappropriate manner.

This Acceptable Use Agreement is intended to ensure:

- That students understand how to be responsible users and stay safe while using the internet, IT systems and other communication technologies for educational, personal and recreational use.
- That the RSA's systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk. Students will have access to IT and Communications systems to enhance their learning. In return, RSA expects students to agree to be responsible users.

The use of the RSA systems is a privilege and inappropriate use can result in that privilege being withdrawn. To qualify for access to the RSA's IT and Communications systems, students must read, sign and return this Agreement.

CODE OF CONDUCT

Equipment Security and Passwords

- I will keep my username and password to myself. I will not use any other person's username and password and I will not allow anyone else to use my username and password. I will always keep my passport secure and I understand that I should not write down or store a password where it is possible that someone else may see or have access to it.
- I will not attempt to move or tamper with any Desktop PCs, cabling for telephones or other computer equipment without first consulting a member of staff.
- I will not attach any device or equipment to RSA's systems without the prior approval of a member of staff. This includes any USB storage devices, mobile phones, tablet computers or PDAs. It also includes use of the USB port, infra-red connection port or any other port.
- I will not deliberately damage any RSA equipment.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Online Safety

- I will be aware of contacting and being contacted by strangers whilst communicating online.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I will not remove safety filters from Internet search engines in order to access unsuitable or restricted material.
- I will not use online messaging or "chat" services, unless I have permission from a member of staff. This includes the use of the Office 365 chat functions.

Behaviour

- I understand that RSA's systems and devices are primarily intended for educational use and I will not use them for personal or recreational use unless I have permission from a member of staff.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work. I will always seek permission before downloading or uploading anything I am unsure about.
- I will not use the RSA's systems or devices for online gaming, online gambling, file sharing, video/audio broadcasting or streaming (e.g. YouTube) or instant messaging, unless I have permission of a member of staff to do so.
- I will not install or attempt to install or store software or programmes of any type on any RSA device, unless I have permission of a member of staff to do so.
- I understand that any incoming files and data should always be virus-checked before they are downloaded.
- I will not delete, destroy or modify existing systems, programs, information or data which could cause damage to RSA or its systems, or expose them to risk.
- I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without that user's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language. I appreciate that other people may have different opinions to me and I will be respectful of those opinions.
- I will not take or distribute images of anyone without their permission.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not attempt to gain access to restricted areas of the systems, or to any password-protected information, without prior permission.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email. If I have any suspicions about the validity or source of an email, I will report this to a member of staff.
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I will only use social media sites with permission from a member of staff and at appropriate times which will be indicated to me from time to time by RSA.
- I will not use the RSA's systems for ordering goods or services without permission from a member of staff. I also understand that it is forbidden to subscribe to any newsletter, catalogue or other form of correspondence via the Internet unless I have permission.
- I will use Office 365 appropriately, in particular Outlook and Teams. I will not create unnecessary teams and will not post inappropriate content onto any application in Office 365.

Monitoring

- I understand that the RSA's systems enable RSA to monitor telephone, e-mail, voicemail, internet and other communications. For legitimate reasons, and in order to carry out legal obligations in the RSA's role as an education services provider, use of the RSA's systems including the telephone and IT systems, and any personal use of them, is continually monitored by the RSA's external IT provider. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for legitimate purposes.
- I understand that emails are not guaranteed to be private and RSA monitors all e-mails passing through its system for viruses. I understand that RSA may need to retrieve the contents of e-mail messages, communications on Office 365 or check internet usage as reasonably necessary in the interests of the RSA, including but not limited to the following purposes:
    - to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this Acceptable Use Agreement;
    - to find lost messages or to retrieve messages lost due to computer failure;
    - to assist in the investigation of alleged wrongdoing; or
    - to comply with any legal obligation.
- Messages relating to, or in support of, illegal activities may be reported to the appropriate authorities.

Use of Personal Devices

- I will only use my own personal devices in the RSA if I have permission. I understand that, if I do use my own devices in RSA, I will follow the rules set out in this Agreement in the same way as if I was using the RSA's equipment.

- During lessons my own personal devices should be put away. I understand that if I use my own personal device in lessons it will be confiscated until the end of that College day. Continued misuse of personal devices may result in me being banned from having personal devices in RSA.

Personal Responsibility

- I understand that I must use the RSA's systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. ,
- I will report any misuse of the RSA's systems to a member of staff. I understand that misuse may come in many forms – this can include any messages sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence and attempts to disrupt or hack into the computer network.
- I understand that RSA has the right to take action against me if I am involved in misuse or incidents of inappropriate behaviour covered by this Agreement. This includes when I am outside of the RSA, where the incidents involve my membership of the RSA community.
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the RSA's systems / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

DECLARATION

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to RSA's systems.

Name of Student: .....

Group / Class: .....

Signed: .....

Date: .....

Parent / Guardian Countersignature (optional)