INFORMATION AND COMMUNICATIONS TECHNOLOGY ("ICT") & E-SAFETY POLICY

The Rodillian Multi Academy Trust

Summary	ICT & E-Safety Policy		
Responsible Person/Author:	Director of IT and Data Human Resources Director Head of Governance and Compliance		
Applies to: (please circle/delete as appropriate)	**Staff ☒**	**Student☒**	**Community ☐**
Ratifying Committee(s)	RMAT Board		
Available On:	SharePoint, Website, On Demand		
Date of Approval	29 August 2024		
Effective from:	30 August 2025		
Date of Next Formal Review:	August 2025		
Review Period	1 Year		
Status:	Statutory		
Owner	The Rodillian Multi Academy RMAT		
Version:	3		

Document Control

Date	Version	Action	Amendments
20.11.21	1	Policy reformatted	
10.22	2	Policy amended	
07.24	3	Policy amended	Added sections on generative AI

Contents

Introduction

1. This document sets out RMAT's policy for the use of ICT devices, systems and peripherals connected to RMATs networks. These include:

    - Fixed computers in offices and classrooms;
    - RMAT provided laptops, tablets, and phones;
    - RMAT email and digital communication systems;
    - RMAT Cloud systems;
    - Remote access solutions to RMAT networks and
    - RMAT digital cameras, camcorders, and audio recorders.
    - Personal devices connected to RMAT networks (See separate Bring Your Own Device (BYOD) guidance)

2. This policy explains the behaviours, which are acceptable and unacceptable with regard to use of ICT in the RMAT.

Scope and Purpose of this policy and who it applies to

2. This policy applies to all who use or access RMAT ICT systems including members of RMAT Governance, RMAT employees, Third Party Contractors who may need access to the RMAT ICT systems and students. The policy will be brought to the attention of all employees as part of their induction. Non-compliance with this policy by employees may lead to disciplinary action being taken against them.

3. The RMAT is also the sole shareholder in the company known as Southway at the Rodillian Academy Limited (Company number 08492483) ("Southway") which operates the Southway Key Stages 3 and 4 extended educational provision. This policy applies to Southway (an Independent School), its employees, directors, third party contractors and students who access Southway or RMAT ICT systems as if it was an RMAT Academy.

4. All users should note that ICT systems and internet use are monitored on a regular basis. Any user who is found to deliberately infringe this policy may be subject to disciplinary procedures or legal action.

5. This policy also refers to staff's personal use of the internet (on and off-site) though social media and other forms of digital communication, including use of personal mobile devices.

Publication of this policy

6. This policy will be brought to the attention of all staff and members of RMAT Governance and will be available to them to read as needed. Following any amendment or replacement of this policy, an updated version will be made available to all staff, and they will be advised by email where they may access the amended or replaced policy.

7. Guidance on any aspect of this policy can be obtained from the Head of Governance and Compliance. amarham@rmat.uk

Responsibility for this policy

8. The RMAT Board has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory or RMAT framework. RMAT has delegated day to day responsibility for operating this policy to the RMAT Executive.

Aim of this Policy

9. To regulate the use of RMAT ICT systems and devices.

Online Safety

10. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

11. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Unlawful and Illegal Material

12. Illegal material includes the depiction of the abuse of children and young people, race hatred and incitement to violence. This list is not exhaustive and there may be other information that is deemed to be illegal.

13. Accidental access to material, which may be classed as illegal should be reported to the Internet Watch Foundation ("IWF") – **www.iwf.org.uk** as well as directly to the Academy Principal or in the case of Central Services staff or members of Governance the Data Protection Officer or Director of ICT and Data.

14. If you receive images or content including sound files, which you believe could be illegal it is imperative that you make no attempt to investigate the content. A written signed and dated log of the incident should be made to show that there is suspicion of inappropriate or illegal material. This log is to protect you from any suspicion for having potential illegal material in your possession. This log should then be submitted to the Academy Principal or in the case of Central Services staff or members of Governance the Data Protection Officer or Director of ICT and Data. Once this log has been made the Uniform Report Locator ("URL") if appropriate should be reported to the IWF. This must be done by typing the URL address into the report not by copy and paste. It is possible to accidentally open a link so care must be taken.

15. If the content is an image in the body of an email, close the email and make a log of the incident as above. A report should be made to the IWF. They will advise what to do next. Under no circumstances forward the email, copy the image, or show it to another person, as each of these actions may constitute a criminal offence. The IWF, is licensed to investigate, you are not. For guidance in this area refer to a member of the Academy leadership team.

16. As a user of ICT within RMAT you agree not to use the ICT facilities to create, send, or receive materials or data, which are:

- in violation of any law or regulation;
- which is defamatory, offensive, abusive, indecent, obscene;
- which constitutes harassment;
- is in breach of confidence, privacy, trade secrets;
- is in breach of any third-party Intellectual Property rights (including copyright);
- is in breach of any other rights or has any fraudulent purpose of effect.

17. You are prohibited from storing, distributing, transmitting, or permitting the storage distribution or transmission (whether intentionally or otherwise) of any unlawful material through RMAT systems.

18. Examples of unlawful material include:

- Direct threats of physical harm
- Child abuse images
- Incitement to racial hatred
- Copyrighted, trademarked and other proprietary material used without proper authorisation.

19. You may not post, upload, or otherwise distribute or permit the posting, uploading or distribution (whether intentionally or otherwise) of copyrighted material on RMAT servers without the consent of the copyright holder.

20. The storage, distribution, or transmission of unlawful materials could lead to criminal prosecution or civil proceedings being taken against you.

Inappropriate use of RMAT ICT systems

21. Inappropriate use of the network includes accessing or having possession of material that is thought to be offensive including but not limited to, adult pornography of any level or content of an obscene, indecent and/or abusive nature. You should be aware that disciplinary and/or civil action might arise if users are found to be accessing material of this nature across the RMAT network.

22. Staff must **NOT** have any form of social contact via the internet with current or former students. Staff should be aware that in the event that this is found to have happened disciplinary action will be taken.

23. Staff must **NOT** name their employer on any social networking site with the exception of LinkedIn, as this could potentially bring the RMAT into disrepute. Staff should be aware that in the event that this is ignored, where there are issues arising from this, disciplinary action will be taken.

24. All communication carried out over RMAT ICT systems should be conducted in a professional manner.

Security and Protection

25. It is the responsibility of all staff to protect the physical safety, and e-safety of students when using any ICT facilities of RMAT. All users of RMAT ICT systems are required to be individually identifiable. This means that every user of the network must have an individual username and password. This must be securely kept and not passed onto other users. **In the event of an investigation into misuse, proper use of passwords will protect innocent users from the upset and embarrassment of suspicion for inappropriate or illegal misuse.**

26. All personal social media content must be protected with the correct privacy settings. Under no circumstances should adult users share content, link your profiles, or allow your content to be shared or linked with current or former students. Please also give consideration to any wider personal publicly published web content and understand that this may be viewed by students.

27. You should be aware that it is the responsibility of all adult users to ensure that personal privacy settings are always maintained to prevent access from students (current and former). If any issues arise in the absence of secure privacy settings this could result in disciplinary action being taken.

28. Sharing of digital files should be done in a secure manner with an understanding of the nature of the information being made accessible. All resources that are shared externally must follow controls detailed in the Data Protection and Information Governance policy.

E-mail and Digital Communication

29. RMAT, at its discretion has the right to access, review, and copy or delete all information contained in emails or other digital forms of communication held on RMAT networks, and use it as we consider appropriate.

30. Email is not typically encrypted and therefore is potentially insecure particularly when leaving the RMAT network and traversing the internet. Please bear this in mind before including confidential or sensitive information in emails. Furthermore, the internet offers no guarantees of delivery of the email. Ask for further guidance from ICT support staff if you need a secure information transfer.

31. Bear in mind at all times that your and others' RMAT network use, internet and email use could be monitored. Deleting an email, message, or file from your computer is not the same as throwing away a sheet of paper. It will be possible for the RMAT to retrieve it.

32. **Always:**

- assume that whatever you put in an email or other digital communication may have to be disclosed to the police, in court proceedings or to regulatory bodies;

- ensure that when you are away from the academy and unable to respond for any length of time you switch on 'Out of Office' and/or make sure emails addressed to you are read by a colleague who knows how to respond (emails can be forwarded automatically for this purpose). If setting an Out of Office message think about the information you are sharing such as that you are on holiday as this may be used by cybercriminals to send colleagues a phishing email. An example out of office message is.

  "I am out of the office until x date. I will/will not be accessing my emails intermittently during this time. If this matter is urgent, please contact .”

- make sure email messages are subject to the same level of supervision as letters;

- remember that emails or other digital communication can constitute/contain personal data under the UK General Data Protection Regulation ("GDPR") and should be dealt with in accordance with rules relating to personal data in general.

- include an email auto-signature to include your name, position and/or department and contact details (telephone and email address).

- Any necessary authorised communication with students and parents/carers should be via your RMAT email account and **not** any personal email account. The use of personal emails to contact students/parents/carers will lead to disciplinary action been taken by RMAT and may lead to criminal prosecution.

33. **Do not:**

- send abusive, obscene, sexist, racist, language/text which demeaning of those with disability or relative social, economic, or educational disadvantage, harassing, defamatory, suggestive, or improper/unwise in the context of the welfare of young or vulnerable person's messages or images;

- use the RMAT email system for an unlawful purpose;

- send messages from a colleague's computer or send messages in another's name (unless you have been asked to do so by that person in writing and it is work related), in these circumstances it must be made clear that the email is sent for and on behalf of the colleague;

- open unknown or odd-looking emails or attachments without having them checked for viruses;

- create excessive and unnecessary email traffic by failing to keep the number of email addresses to a minimum, or by sending personal emails to several recipients; e.g. by forwarding jokes or sending emails for advertising. The RMAT email system is not to be used for any purpose unconnected with the business of RMAT without express permission from a designated senior leader;

- send confidential or sensitive information to those who are not its proper recipients;

- infringe third party intellectual property rights by including infringing material in an email or by forwarding an email containing such material;

- use a personal email account or other digital communication platforms to correspond in connection with RMAT matters. Personal email accounts neither provide the audit trail which is necessary nor include the standard disclaimers;

- communicate with students via a personal email account or digital communication platform.

- give anyone else your passwords. This includes checking that login attempts are on genuine sites and pages. Most phishing techniques involve tricking the target into thinking they are logging in to a different service and therefore compromising their own credentials.

Rules for the Use of RMAT ICT systems by Students

34. ICT systems used in the RMAT are owned by RMAT and are solely made available to students to further their education. RMAT reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited; emails and messages sent and received using the internet.

35. RMAT will not be liable under any circumstances for any injury, distress, loss or damage to the student or the parents, which may arise directly or indirectly from the student's use of the ICT facilities, the use of e-mail, or from a student's unauthorised use of those facilities or e-mail.

36. Students must abide by the following rules when using RMAT owned ICT devices and systems:

- Access to the computers and the internet must only be made via an authorised RMAT username and password. Students must not use a username and password that is not their own;

- All internet use should be appropriate to a student's education. Sites and materials accessed must be appropriate to work set in RMAT academies;

- The downloading of sexist, racist, pornographic, indecent, or abusive images, text or sound files is forbidden;

- The downloading of any program, screen saver, game etc. without permission from an authorised member of staff is forbidden;

- The downloading of music or video is forbidden unless special permission has been obtained;

- Activity such as hacking, virus writing, disabling security software or any other activity that threatens the integrity of RMAT ICT systems, or that attacks or corrupts other systems, is forbidden;

- Users are responsible for e-mail and messages they send and for contacts made that may result in e-mail and messages being received;

- RMAT academies insist that students do not use language or materials on their emails, messages or computer work that others will find abusive or threatening;

- Posting anonymous messages and forwarding chain letters is forbidden;

- Copyright of materials and intellectual property rights must be respected;

- Purchases over the Internet are forbidden;

- Computer or Internet use for personal financial gain, gambling, political purposes, or advertising is forbidden;

- Removal of any computer identification is forbidden;

- Contacting or searching for members of staff through social media sites is not permitted.

- Using generative AI platforms to create non-exam assessment for qualifications is prohibited and will be considered malpractice as per the Joint Council for Qualifications (JCQ) regulations.

Rules for the protection of Hardware and Supervision of Student Access

Protection of Hardware

37. It is the responsibility of every department in an Academy to ensure the correct and safe use of ICT devices assigned to them to ensure that teaching and learning is not detrimentally affected. This includes referring maintenance issues using the correct procedures in the Academy:

- When not in use laptop/tablet trolleys should be locked.

- When not in use/unsupervised laptop/tablet trolleys should be locked in a classroom or office.

- Laptops/tablets should be stored in the trolleys provided and plugged in to charge to ensure ease and efficiency of use.

- If sharing trolleys or laptops/tablets it is the responsibility of all teachers involved to return them before the end of the lesson.

- Students should not carry laptops by the screens or have fingers on the screens.

- Care should be taken when moving trolleys around the academy and this should be supervised by staff.

Supervision of Student Access

38. Teachers and other staff are responsible for:

- The monitoring of student ICT activity in lessons, extra-curricular and extended Academy activities.
- Remind students of how to use the internet safely and where/how to report any concerns.
- Remind students of how to use the internet safely and where/how to report any concerns.
- Taking an active role as appropriate in promoting safe internet and technology usage and discussing the risks facing students online.
- Never use or share personal ICT devices on site with students or allow students to use their own personal ICT devices on site.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use.
- In lessons where students are allowed to freely search the internet, e.g. using search engines, teachers should be vigilant in monitoring the content of the websites' students visit.
- 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, staff can request that the ICT support team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be in writing or via email with clear reasons for the need.

39. It is good practice to

- Identify rooms for numbered trolleys to be stored and returned to.
- Identify a member of the department or corridor to take responsibility for certain trolleys.
- Have a booking system for Departments/corridors.
- Laptops/tablets are returned from the trolley from which they came.
- Choose a student to act as Trolley monitors in lessons (this has proven to work well in some lessons with appropriately chosen students).

- Spot check ICT facilities at the beginning and end of your lessons to monitor for any vandalism.

- Use a seating plan in ICT Classrooms to easily identify which students have used which devices.

- 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.

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

- Students should be taught about the dangers of using the internet and how they should conduct themselves online.

- Be aware of student use of generative AI and consider whether any digital work students produce may have been created in this manner.

Use of Digital Images and Video

40. 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. Staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

41. 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.

42. Staff are allowed to take digital / video images to support educational aims but must follow RMAT policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on RMAT equipment; the personal equipment of staff should not be used for such purposes.

43. 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 RMAT into disrepute.

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

45. Photographs published on the RMAT or an Academy website, or elsewhere that include students must be selected carefully and will comply with good practice guidance on the use of such images. This includes having sought parental permission for any images of students used publicly. Staff should bear in mind how long it is appropriate for an image to remain on a website or other RMAT platform especially following the student leaving the Academy.

46. Staff must not use personal devices to share digital images which could be deemed as inappropriate.

Use of Generative Artificial Intelligence (AI)

47. The use of generative AI in education has both opportunities and concerns. For example, it can:

- Create realistic and engaging content for learners, such as text, images, audio, or video, based on their preferences and needs.
- Save time finding information or imagery required for planning and lesson materials.
- Automate the creation and evaluation of assessments, as well as provide feedback and scoring for learners' responses.
- Enhance the diversity and inclusivity of educational materials, by generating content that reflects different cultures, languages, perspectives, and backgrounds.

However, staff and students should be aware that it can:

- Pose ethical and social challenges, such as the potential misuse of generated content for malicious or deceptive purposes, or the infringement of intellectual property rights or privacy.
- Raise quality and reliability issues, such as the accuracy, validity, and relevance of the generated content, or the possible biases or errors in the generation process.
- Require technical and pedagogical skills, such as the ability to evaluate, interpret, and integrate the generated content, or the knowledge of how to use and teach with generative AI tools.
- Be used by students to create work, which is not their own, including non-exam qualification content which would fall under malpractice with the JCQ regulations.

Staff should be aware of these opportunities and concerns and follow the appropriate guidelines and policies when using generative AI in education.

48. Staff should use the RMAT cloud platform for generative AI wherever personal or confidential information is being used in the prompts. When used in conjunction with the user's login the platform offers commercial data protection. Where this is not the case, any prompts and responses are being used to train the system and any information included can be used in responses for anyone else using that platform.

Data Protection

49. Personal data will be recorded, processed, transferred, and made available according to GDPR which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant, and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.

- Secure.
- Only transferred to others with adequate protection.

50. Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use or store personal data only on secure password protected computers or other devices, ensuring that they are properly logged-off or locked at the end of any session in which they are using personal data.

- Transfer confidential or sensitive data using encryption and secure password protected devices.

- Share any digital files in a secure manner with an understanding of the nature of the information being made accessible and the audience being granted access.

- Don't use prompts with generative AI that includes personal or confidential information where the platform does not support commercial data protection.

51. All staff are expected to complete a short training programme on Data Protection. This will cover the basics of GDPR and the individuals' responsibility for protecting the personal data RMAT holds. If individuals are found to be in minor breaches of areas of the ICT or Data Protection policies, then additional mandatory training packages will be targeted at staff.

Online and Remote Learning

52. Online teaching of lessons for students should follow the same principles as set out in the RMAT's Safe Working Practice Policy which contains guidance for those working with children and young people in education settings (National Safer Recruitment Consortium May 2019).

53. RMAT will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

54. Whilst staff are interacting with children away from the academy online, they must continue to adhere to RMAT's Personal and Professional Conduct of Staff, Safe Working Practice Policy, ICT and E-Safety Policy and any other policies, protocols, professional standards, and statutory guidance applicable to their role.

55. Staff should use parents' or carers' email addresses or phone numbers from the academy management information system (SIMs) or academy parental engagement technologies to communicate relevant information about children, unless this poses a safeguarding risk. Use work accounts to communicate via email or online platforms, **never use personal accounts.** All remote communication with students should be done exclusively via academy/centre approved IT platforms.

56. Staff are able to access or download RMAT platforms with personal devices but must ensure that **any devices used are securely password or biometrically protected.**

57. If staff members are accessing families' contact details at home, ensure they comply with the Data Protection Act 2018.

58. Delivering remote lessons

- Remote 1:1's with students should be avoided, with students being tutored in groups wherever possible. If this is unavoidable, this must be approved by the Academy Principal.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; staff need to be mindful that backgrounds do not compromise personal confidentiality or breach the guiding principles of safer working practice guidance for staff working in educational settings.
- Live classes should be recorded so that if any issues were to arise, the video can be reviewed.
- Language must be professional and appropriate, including any family members in the background.
- Staff should monitor any class peer to peer conversations through remote learning platforms where possible.
- Staff must only use platforms specified by senior leaders and approved by the RMAT IT Director to communicate with students.
- Records should be kept of the length, time, date, and attendance of any sessions held.
- Consider activities carefully when planning – online access within school has internet content filtering systems in place that are unlikely to be replicated in the home environment.
- Be careful that staff and children don't incur surprising costs, e.g. mobile data access charges - (video utilises significant amounts of data).

E-Sports

59. E-Sports is short for electronic sports which are organized competitive video gaming. From time to time, students (predominantly at UTC Leeds) will take part in E-Sports.

60. Staff who supervise/lead students in E-sports should ensure:

- Students are aware who they are interacting with online and what to do if anything inappropriate is said to them or anyone engages in cyberbullying.
- Games played by students are age appropriate and students should play them responsibly, politely whilst respecting others both on and offline.
- Students should be careful about sharing personal information

- That students should play e-sports in a balanced way and employ healthy gaming habits.

- That students should communicate to staff and/or their parents any issues encountered whilst playing e-sports including but not limited to inappropriate behaviour, cyberbullying or other concerns.

- That the use of chat functions should be supervised by a member of staff, i.e. headphones should not be used.

61. E-sports played in RMAT academies will be subject to our usual filtering and monitoring controls.

62. Parents should ensure appropriate parental controls are in place for e-sports played at home.

Reporting concerns

63. Communicating online may allow you a view into a young person's world that you would not have seen before. This may also generate some safeguarding concerns for that young person. It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Any concerns must be recorded and monitored on CPOMS, and a Designated Safeguarding Lead (DSL) must be informed immediately.

64. You will also notice if a child is not engaging in learning as required. Where this is the case, after an agreed period of time in line with your academy agreed protocol, this must be reported to a member of the Leadership team so that contact can be made with the child and parent/carer to ensure they are safe and well.

Appendices

65. To support staff and students in clearly understanding the key ICT and e-safety rules and their responsibilities in regard to this policy there are Acceptable Usage Policies attached below.

66. Staff and students are expected to have read and understood these Acceptable Usage Policy documents, which outline their personal responsibilities as outlined in this policy.

Appendix 1: Staff ICT use Policy

1. Never disclose your password to anyone. Never use someone else's logon details or password or allow anyone else to use your logon details.

2. Under no circumstances should you view, upload, or download any material which is likely to be unsuitable for children. This applies to any material of a violent, dangerous, sexual, or inappropriate nature.

3. To protect yourself and the RMAT ICT systems, you should respect the security of RMAT networks; attempting to bypass or alter the settings may put you or your work at risk.

4. Always get permission before installing, attempting to install, or storing programs of any type on RMAT networks.

5. Do not download, use, or upload any material which is in breach of copyright.

6. Do not give out the personal information of any member(s) of staff or student(s) from RMAT without the correct authority to do so.

7. You must ensure that any personal data belonging to students or staff, that you send externally from RMAT, or you take offsite is securely encrypted and used appropriately in line with the RMAT's Data Protection and Information Governance Policy.

8. You must ensure that any sharing of digital files is done in a secure manner with an understanding of the nature of the information being made accessible and the audience being granted access.

9. Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed.

10. Always respect the privacy of files of other users. Do not modify files in common areas unless they belong to you, or you have received express permission.

11. Personal storage drives and emails on the RMAT network or on Office365 are not private. RMAT staff may be required to access your files/communications to ensure that the systems are being used responsibly.

12. Arrange for suitable monitoring of students in your class, or those students who you have given permission to use the ICT facilities.

13. Protect the computers from spillages by eating or drinking well away from the ICT equipment.

14. Only open attachments to external emails if they come from someone you already know and RMAT. Attachments can contain viruses or other programs that could destroy files and software on held on RMAT networks.

15. Never leave a workstation logged on and unattended. Use the 'Lock Computer' (press the Windows Key + L) function if you need to leave a workstation for a short period of time. This applies both in academy and whilst accessing the academy network remotely.

16. When remotely accessing the RMAT network or systems on shared devices, never allow the local computer/device to automatically remember and enter the username and password.

17. Report any incident which breaches the Acceptable Rules Policy immediately to the ICT Support Team. This includes any misuse by students.

18. All communication with students, parents/carers, and the wider public should only be carried out using RMAT equipment and systems. This includes not using personal telephone numbers, email accounts, or social networking sites.

19. All communication carried out over RMAT ICT systems should be conducted in a professional manner.

20. All personal social media content must be protected with the correct privacy settings. Under no circumstances should you share content, link your profiles, or allow your content to be shared or linked with students. This includes students who have left the Academy. Please also give consideration to any wider personal publicly published web content and understand that this may be viewed by students.

21. Staff must **NOT** have any form of social contact via the internet with current or former students. Staff should be aware that in the event that this is found to have happened, disciplinary action will be taken.

22. Staff must **NOT** name their employer on any social networking site except LinkedIn, as this could potentially bring RMAT into disrepute. Staff should be aware that in the event that this is ignored, where there are issues arising from this, disciplinary action will be taken.

23. No personal devices should be used with or given to students or parents/carers. This includes mobile phones, cameras, camcorders, and storage devices.

24. No personal data storage devices or personal cloud storage providers should be used. This includes personal photography or recording equipment.

25. Ensure that any tablet device or mobile phone that you use to integrate with the Academy systems is passcode protected.

26. Only use RMAT platforms for generative AI where you are using prompts that contain personal or confidential information.

27. Misuse of ICT may lead to disciplinary action being taken against you.

I have read the above and understand my roles and responsibilities.

Name _____ Signature _____ Date _____

Appendix 2: Student ICT use Policy

1. Never disclose your password or logon name to any other student or anyone else. Never use someone else's logon details or password or allow anyone else to use your logon details.

2. Never leave a workstation logged on and unattended. This applies both on site and whilst accessing the Academy network/systems remotely.

3. Do not give out any personal information over the Internet and always respect the privacy of other users.

4. You should access the Internet only for study or for Academy authorised/supervised activities. You may only use the internet during curriculum time as specified by a member of staff.

5. Do not download, use, or upload any material which is in breach of copyright.

6. Do not view, upload, or download any material which is likely to be unsuitable. This applies to any material of a violent, dangerous, sexual, or inappropriate nature.

7. Do not upload or create material on the Internet or the Academy network, either in or out of school, which may cause offence to any members of the school community or damage the Academy reputation.

8. Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Cyber Bullying is never tolerated, and it is not acceptable to behave in a manner which is intimidating, threatening or in any way discriminatory to another student either in or out of the Academy site.

9. Protect the computers from spillages by eating or drinking well away from the ICT equipment.

10. To protect yourself and the systems, you must respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.

11. Personal IT storage areas accessed from your Academy account, including on the Cloud and emails, are not private. ICT support staff may need to view your files to ensure that the system is being used responsibly.

12. Only open attachments to external emails if they come from someone you already know and RMAT. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

13. All Academy ICT systems are monitored, and use is fully logged. This includes on Academy owned devices for home use, or through remote access or cloud services.

14. No personal devices should be used onsite in conjunction with the Academy ICT. This includes mobile phones, cameras, camcorders, and storage devices.

15. When taking part in a remote lesson please be aware of your surroundings particularly when using a camera. Remote lessons may be recorded.

16. Contacting or searching for members of staff through social media sites is not permitted.

17. People you contact on the Internet are not always who they seem. Never go to meet someone who you only know from the Internet or via email.

18. Using generative AI and pretending the work is your own is cheating and is considered serious malpractice under the exam boards regulations if used for non-exam assessment as part of any qualification.

19. Report any incident which breaks this acceptable use policy immediately to a member of staff. This includes any misuse by other students.

Failure to comply with these rules may result in:

- **A ban, temporary or permanent, on the use of the Internet or ICT facilities at the Academy.**
- **A letter informing your parent/carer of the nature and breach of rules.**
- **Additional action in line with existing policy regarding Academy behaviour.**

For serious violations, a suspension or permanent exclusion may be imposed. Where appropriate, police may be involved, or other legal action taken. If you do not understand any part of this Acceptable Use Policy, you must ask a member of staff.