e-Safety and Cybersecurity Policy

This document has not yet been formally ratified by RAK Academy Board of Governors but has been released for implementation. Document No. POL25.110520.A-16

1. Rationale

This policy provides guidance and directions on e-Safety and cybersecurity for stakeholders, both inside and outside the Academy.

While modern technology offers many social and academic benefits for teaching and learning by allowing individuals to share ideas and exchange information, it is important to understand the potential harm that can be caused by its misuse and there are risks associated accordingly. These include legal risks under the UAE laws and the personal liability that may arise from misuse or lack of consideration when posting online or undertaking other activities on the Internet.

The purpose of this policy is to:

- Set out the key principles expected of all members of the RAK Academy community with respect to the use of computer-based technologies
- Safeguard and protect the students and staff of RAK Academy
- Assist staff working with students to work safely and responsibly with the Internet and other communication and collaboration technologies and to monitor their standards and practices
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational purposes
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other Academy policies
- Ensure that all members of the Academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action may be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students

2. Scope

This policy applies to all members of the Academy community including staff, students, parents/guardians and visitors who have access to and are users of the Academy computing systems, both in and out of the Academy. This policy also applies during periods of Distance Learning and includes interactions between stakeholders.

3. Risk Areas

The main areas of risk for our community can be summarised as follows:

Content:

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), and substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites/hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact:

- Predatory grooming
- Online bullying in all forms
- Identity theft (including hacking social media profiles) and sharing passwords

Conduct:

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming))
- Sexting (sending and receiving of personally intimate text or images)
- Any forms of extremism
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

4. Roles and Responsibilities

The following table describes different roles together with key responsibilities:

Role	Key Responsibilities
Executive Principal and Head Teachers	• Take overall responsibility for e-Safety and cybersecurity provisions • Ensure the Academy uses an approved, filtered Internet Service, which complies with current statutory requirements • Responsible for ensuring that staff receive suitable training to carry out their e-Safety and cybersecurity roles and to train other colleagues, as relevant • Aware of procedures to be followed in the event of a e-Safety and cybersecurity incident or Internet security breaches • Receive regular monitoring reports from the e-Safety and Cybersecurity Co-ordinator and help plan a course of action as needed • Ensure that there is a system in place to monitor and support staff who carry out internal e-Safety and cybersecurity procedures (e.g. IT Manager) • Ensures technology infrastructure and data systems support the aims of this policy
Designated Child Protection (CP) Officer	• Takes day to day responsibility for e-Safety and cybersecurity issues arising and has a leading role in establishing and reviewing the academy e-Safety and Internet Security policies/documents • Promotes an awareness and commitment to online safeguarding throughout the Academy community • Ensures that e-Safety and cybersecurity education is embedded across the curriculum • Liaises with Academy IT staff • Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety and cybersecurity incident • Ensures that an e-Safety and cybersecurity incident log is kept up to date • Facilitates training and advice for all staff • Regularly updates themselves in e-Safety and cybersecurity issues and legislation, and be aware of the potential for serious student protection issues to arise from: ○ Sharing of personal data ○ Access to illegal/inappropriate materials ○ Inappropriate on-line contact with adult/strangers

Role	Key Responsibilities
	○ Potential or actual incidents of predatory grooming ○ Online bullying and use of social media
e-Safety and Cybersecurity Board Member	• Supports the Academy in encouraging parents and the wider community to become engaged in e-Safety and cybersecurity activities • Periodically and sporadically reviews e-Safety and cybersecurity artefacts (including e-Safety incident logs, filtering/change control logs) with the e-Safety and Cybersecurity Co-ordinator • Ensures there is a clear roadmap for the storage, access and use of data to enhance learning
Pastoral/ Curriculum Leader	• Oversees the delivery of the e-Safety and cybersecurity element of the curriculum • Liaises with the designated CP Officer
Network Manager	• Reports any e-Safety and cybersecurity related issues that arise, to the e-Safety and Cybersecurity Coordinator • Ensures that users may only access the Academy's networks and systems through an authorised and properly enforced password protection policy and implementation, in which passwords are regularly changed • Ensures that provision exists for misuse detection and malicious attacks e.g. keeping virus protection up to date • Ensures the security of the Academy IT system • Ensures that access controls/encryption exist to protect personal and sensitive information held on Academy-owned devices • Ensures that the Academy's policy on web filtering is applied and updated on a regular basis • Helps keep the Academy's e-Safety and Cybersecurity policy and technical information up to date in order to effectively carry out their e-Safety and cybersecurity roles and informs and update others as relevant • Ensures that the use of the network/Learning Management System/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-Safety and Cybersecurity Co-ordinator/Head Teacher for investigation, actions, or sanctions as appropriate • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • Ensures that critical data of the Academy is stored off-site to support disaster recovery • Keeps up-to-date documentation of the academy's online security and technical procedures
Timetabling and Data Manager/IT Manager	• Ensures that all data held on students on the Academy office computers have appropriate access controls in place
Teachers	• Embed e-Safety and cybersecurity issues in all aspects of the curriculum and other Academy activities • Supervise and guide students carefully when engaged in learning activities involving online technology including, extra-curricular and extended Academy activities as relevant and applicable • Ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• Read, understand and help promote the academy's e-Safety and Cybersecurity policy and guidance

Role	Key Responsibilities
	• Be aware of e-Safety and cybersecurity issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Academy policies with regard to these devices • Report any suspected misuse or problem to the e-Safety and Cybersecurity Coordinator • Maintain an awareness of current e-Safety and cybersecurity issues and guidance e.g. via CPD • Models safe, responsible and professional behaviours in their own use of technology inside and outside the Academy including during web conferencing • Ensure that any digital communications with students should be on a professional level and only through Academy-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. • Ensures that all Academy content including resources (text, audio, images, video, etc.), recordings (such as from live streaming or pre-recorded videos or audios), and artefacts with student data (such as photographs, videos, etc.) are stored only on storage devices or Cloud spaces controlled by RAK Academy
Students	• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology • Know and understand Academy policy on the use of mobile phones, digital cameras and hand held devices • Know and understand Academy policy on the taking/use of images and on cyber bullying • Understand the importance of adopting good e-Safety and cybersecurity practices when using digital technologies inside and outside the academy e.g, during web conferencing and realise that the Academy's e-Safety and Cybersecurity policy covers their actions inside and outside the academy • Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in the Academy and at home
Parents/ Guardians	• Support the Academy in promoting e-Safety and cybersecurity and endorse the students' use of the Internet, video images and web conferencing • Consult with the Academy if they have any concerns about their students' use of technology

5. Communication and Use of the Policy

Communication:

The policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the Academy website/Learning Management System
- Presentations to students, staff and parents

Dealing with Incidents Arising:

Staff and students are given information about infringements in use and possible sanctions. Sanctions and actions available include:

- Interview/counselling by tutor/Intervention Leaders/CP Officer/Head teacher

- Entry onto the most appropriate stage of the Behaviour Policy (depending on perceived and proven severity)
- Deleting inappropriate comments, removing content from an online forum, removing participants from a class and/or escalating concerns in accordance with the Academy policies
- Reporting inappropriate content or comments from online forums
- Informing parents or guardians
- Removal of Internet or computer access for a period
- Referral to Law enforcement agencies

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to student protection are dealt with in accordance with Academy protection procedures.

Use In Conjunction:

Due to the developing and complicated nature of online issues, this policy uses other specific policy frameworks in order to strengthen the Academy's approach. The e-Safety and Cybersecurity policy is referenced from within other Academy policies including the following:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Primary and Secondary Behaviour to Achieve Policies
- Distance Learning Policy

6. Education and Training in e-Safety and Cybersecurity

The Academy has a clear, progressive e-Safety and cybersecurity education and training programme. The programme covers a range of skills and behaviours appropriate to their age and experience, as described below.

Students:

The RAK Academy curriculum embeds e-Safety and cybersecurity aspects for students including the following:

- To STOP and THINK before you CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy
- To be aware that the author of a website page may have a particular bias or purpose and to develop skills to recognise what that may be with reference to the activity being undertaken
- To know how to narrow down or refine a search
- To understand how search engines work and to understand that this affects the results they see at the top of the listings
- To understand how their online activities may be tracked and/or used by unsuspected parties
- To understand acceptable behaviour when using an online environment/email/web conferencing i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
- To understand why they must not post pictures or videos of others without their permission

- To know not to download any files, such as music files without permission
- To have strategies for dealing with receipt of inappropriate materials
- To understand why and how some people will 'groom' young people for sexual reasons
- To understand the impact of cyberbullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying
- To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or guardian, teacher or trusted staff member
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Ensures staff model safe and responsible behaviour in their own use of technology during lessons
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright and intellectual property rights
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming or gambling

Staff and Governor Training:

The Academy:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Provides, as part of the induction process, all new staff with information and guidance on the policy

Parent Awareness and Training:

The Academy runs a rolling programme of advice, guidance and training for parents, including:

- Information leaflets and Academy newsletters on the Academy website
- Presentations and practical sessions held at the Academy
- Suggestions for safe Internet use at home
- Provision of information about national support sites for parents

7. Expected Conduct and Incident Management

Inside and outside the Academy and during periods of Distance Learning, all users:

- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-Safety and cybersecurity practice when using digital technologies inside the Academy and realise that the Academy's e-Safety and Cybersecurity policy covers their actions outside the Academy, if related to their membership of the Academy
- Will be expected to know and understand Academy policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand Academy policies on the use of images and regarding cyberbullying

Staff are responsible for reading the Academy's e-Safety and Cybersecurity policy and using the Academy Computing systems accordingly, including the use of mobile phones, and handheld devices. Students should have a good

understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. Similarly, parents/guardians should provide consent for students to use the Internet, as well as other technologies, and should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management:

Inside and outside the Academy and during periods of Distance Learning:

- There is strict monitoring and application of the e-Safety and Cybersecurity policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the Academy's escalation processes
- Support is actively sought from other agencies as needed in dealing with e-Safety and cybersecurity issues
- Parents/guardians are specifically informed of e-Safety and cybersecurity incidents involving young people for whom they are responsible
- We may refer to Law enforcement agencies if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law

8. Managing the IT and Computing Infrastructure

Internet Access, Cybersecurity, and Filtering:

The Academy:

- Has an educational filtered secure broadband connectivity for students, staff, and visitors. Different filtering policies are applied to these groups of users
- Blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status
- Blocks chat rooms and social networking sites except those that are part of an educational network or approved Learning Management System
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons
- Has blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level
- Uses security time-outs on Internet access where practicable/useful
- Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the Academy's Learning Management System as a key way to direct students to age/subject appropriate websites
- Is vigilant when conducting 'raw' image search with students e.g. Google image search
- Informs all users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the system administrator/teacher. Our System Administrator logs or escalates as appropriate to the Technical service provider
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme
- Provides advice and information on reporting offensive materials, abuse/bullying etc. available for students, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities

Network Management (User Access, Backup):

The Academy:

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short-term visitors for temporary and limited access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where needed
- Has additional local network auditing software installed
- Storage of all data within the Academy will conform to the UAE data protection requirements
- Ensures the network is used safely
- Staff access to the Academy's management information system is controlled through a separate password for data security purposes
- We provide students with an individual network log-in username.
- All students have their own unique username and password which gives them access to the Internet, the Learning Management System
- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves
- Has set-up the network so that users cannot download executable files/programmes
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the Academy provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the Academy, is used solely to support their professional responsibilities and not for their personal use
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access to report writing module etc.
- Ensures that access to the Academy's network resources from remote locations by staff is restricted e.g. teachers access to their areas
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support from ISAMs or via link sharing with a specified expiry date
- Makes clear responsibilities for the daily back up of all management systems including School Management (e.g. ISAMS), Enterprise Resource Management and Finance (e.g. Orison) and other important files

- Requires that a subscription to any website or service is created using a RAK Academy email address and not a personal email account, and that an admin level account is created for it@rakacademy.org or another suitable email account provided by the IT Team
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements
- Uses our broadband network for our CCTV system
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Our wireless network has been secured to industry standard enterprise security levels and appropriate standards suitable for educational use
- All computer equipment is installed professionally and meets health and safety standards
- Projectors are maintained so that the quality of presentation remains reasonable high
- Reviews the Academy IT systems regularly with regard to health and safety and security
- Ensures that access to the systems and the networks of the Academy is promptly removed for staff, students, and parents that are no longer part of RAK Academy community

Password Policy:

- This Academy makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it
- All staff have their own unique username and private passwords to access Academy systems. Staff are responsible for keeping their password private
- We require staff to use STRONG passwords for access into our MIS system including email and ISAMS
- We require staff to change their passwords every 30 days

Email:

The Academy:

- Provides staff with one or more email accounts for their professional use and makes clear that all personal email should be through a separate account of their own
- May contact the Law enforcement agencies if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and are up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of technologies to help protect users and systems in the Academy, including desktop anti-virus software

9. Resources and Content in RAK Academy

Academy Website:

RAK Academy has an update website with content and information for all schools with the following guidelines:

- The Executive Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. The Heads of School are responsible to ensure that the content on the website is accurate and up-to-date ongoing basis
- Uploading of information is restricted to persons specified by the Executive Principal
- Photographs published on the web do not have full names attached or shown

- We do not use students' names when saving images in the file names or in the tags when publishing to the Academy website
- We expect teachers using Academy approved blogs/wikis/any other forms of social media to password protect them and run them from the Academy website as links

Learning Management System (e.g. Google classroom/SeeSaw):

RAK Academy uses multiple Learning Management Systems (LMS). This includes Google Classroom (as part of G Suite for Education) and Seesaw. The Portfolio functionality in ClassDojo is also used as an LMS. The following will apply to LMS used in RAK Academy.

- Uploading of information on the Academy's Learning Management System is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the Academy's Learning Management System will only be accessible by members of the academic community of RAK Academy or by external parties (inspection bodies) where warranted and approved by the Executive Principal
- In Academy, students are only able to upload and publish within Academy approved Learning Management Systems

Social Media:

For the purpose of this policy, *Social Media* is defined as any online interactive tool which allows for interaction, exchanges and for networking. Forms of social media include, but are not limited to, Facebook, Flickr, Instagram, YouTube, LinkedIn, Snapchat and Twitter, as well as blogs, discussion forums, instant messaging such as WhatsApp or iMessage and any website which allows public commenting, viewing or posting.

Social media use in teaching and learning

Social media can often be used as a useful teaching resource as it allows access to a wide range of useful resources and allows connections to be made with experts in various fields of study. Any direct use of social media by teachers with their students should only be permitted from the teacher's professional profile and approved in advance by RAK Academy.

Social media use and personal life

RAK Academy acknowledges that all stakeholders may use social media in their private lives and for personal communications. Personal communications are those made on, or from, a private social media account, such as a personal page on Facebook or a personal blog. In all cases where a private social media account is used which identifies RAK Academy or certain individuals within RAK Academy, this policy will apply. All stakeholders of RAK Academy must be aware of the potential impact and permanence of anything which is posted online. They should understand that digital material posted online can reach wider audiences than was ever possibly expected or intended. Once digital content has been created and shared, there is extremely limited control over its audience.

Expected Standards of Behaviour when using Social Media

The guidelines below provide expected standards of behaviour while using Social Media.

- All stakeholders of RAK Academy are personally responsible for what they communicate on or through social media and must adhere to the standards of behaviour set out in this policy. Additionally, the constraints on such communications imposed by UAE laws and customs should be considered before posting. Under UAE law, defamatory comments about a person, a corporation, a government entity, or a religion may result in severe penalties being imposed, including up to two years in prison. Publishing defamatory comments on social media is no different to doing so in newspapers or books, but the informal nature of social media can catch writers off guard that are not familiar with the sensitivity in the UAE. There have been several high-profile cases in recent years where people have been convicted of defamation after writing insults on WhatsApp, Facebook and Twitter.
- Communications on social media must be respectful at all times and in accordance with this policy and the laws and customs of the UAE. Use of social media must not infringe the rights or privacy of students, parents/guardians,

staff, or any other RAK Academy stakeholders. All stakeholders must refrain from making ill-considered comments or judgments about other students, staff or third parties

- The following non-exhaustive list may, according to the circumstances, be considered to be of an unacceptable nature and should therefore never be posted on social media.
    - confidential information (information about students or staff or personal matters)
    - personal information about another individual, including contact information, without their express permission
    - comments posted using fake accounts or using another person's name without their consent
    - material, including images, that is threatening, harassing, discriminatory, illegal, obscene, indecent, defamatory, or hostile towards any individual or entity connected to the RAK Academy community
    - information that may result in public panic or discord

Video Conferencing:

The Academy:

- Uses Google Meet, Teams, and Zoom for web-based (video and audio) conferences
- While being on a live video or during a recorded video session, teachers should be wearing appropriate attire and select an appropriate background/location. Teachers should also ensure that the recording environment (visual and audio) is professional. One-to-one sessions with students are restricted for counselling purposes only
- It is recommended that all live conferences are recorded for safeguarding purposes
- Teachers should not store recorded live conferences on their personal computers other than temporarily for example during the authoring process. All recordings should be stored in the Google Drive. Teachers should delete recorded sessions (audio or videos) that are no longer needed. The IT Team can recover deleted video files as required. Ensure to use Google Drive associated with your RAK Academy account and not to use your personal Google account

CCTV:

We have CCTV in the Academy as part of our site surveillance for staff and student safety.

- The CCTV recordings are secure and managed by the IT Team
- IT Team will not reveal any recordings without written permission from the Head of School or the Executive Principal
- CCTV recordings should not be used to track items lost by students although it can be used as part of a theft report or a criminal investigation in which case the local police will be involved
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes

10. Data security: Management Information System Access and Data Protection

Strategic and Operational Practices:

- Ensure staff are aware what data needs to be protected and what data can be shared with whom
- Ensure staff are aware who to report any incidents where data protection may have been breached or any protected data has been compromised or where unauthorized personnel gained or were given access to the non-public data about business of the school or about its community members including staff, students, and other stakeholders.

- Ensure staff are aware that any contact with any third party (including vendors, consultants, partners, etc.) must be covered by an NDA (Non-Disclosure Agreement) before any non-public data is shared with them.
- All staff are DBS checked and records are held in one central record with HR
- Academy staff with access to setting-up usernames and passwords for email, network access and Learning Management System access are working within the approved system and follow the security processes required by those systems
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which are no longer needed on the Cloud drives registered under their RAK Academy accounts and on local drives of their RAK Academy computers or other devices. No RAK Academy related content or artefacts should be stored on computers or devices or Cloud based drives not owned by RAK Academy

Technical Solutions:

- Staff have secure areas on the local network or on the Cloud to store documents to store files and other data
- We require staff to log-out of (or screen-lock) systems when leaving their computer
- We require staff to enforce lock-out after 10 minutes idle time
- We store any Protected and Restricted written material in lockable storage cabinets in a lockable storage area
- All servers are in lockable locations and managed by DBS-checked staff
- Paper based sensitive information is shredded

11. Equipment and Digital Content

Students Use of Mobile Phones:

- The Academy strongly advises that student mobile phones should not be brought into the Academy
- Mobile phones and personally owned mobile devices brought in to Academy are the responsibility of the device owner. The Academy accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices
- Student mobile phones which are brought into Academy must be turned off and stored out of sight on arrival at academy. They must remain turned off and out of sight until the end of the day
- Mobile phones will not be used during lessons or formal Academy time unless as part of an approved and directed curriculum-based activity with consent from a member of staff
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited except where it has been explicitly agreed otherwise by the LMT. Such authorised use is to be monitored and recorded
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones
- No images or videos should be taken on mobile phones or personally owned mobile devices without the prior consent of the person or people concerned
- The Academy reserves the right to search the content of any mobile or handheld devices on the Academy premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying, or if the device is used to record unauthorized videos or to take unauthorized pictures.
- If a student breaches the Academy policy then the phone or device will be confiscated and will be held in a secure place in the academy office. Mobile phones and devices will be released to parents or guardians in accordance with the Academy policy

- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an examination will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations
- Where parents or students need to contact each other during the Academy day, they should do so only through the Academy's telephones
- If a student needs to contact his or her parents or guardians, they will be allowed to use an Academy phone. Parents are advised not to contact their student via their mobile phone during the Academy day, but to contact the Academy office
- The Academy accepts that there may be particular circumstances in which a parent wishes their student to have a mobile phone for their own safety
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally owned devices and will be made aware of boundaries and consequences

Students Use of Personal Devices:

Students may bring their own devices complying with the Bring Your Own Device (BYOD) guidelines which include:

- Student passwords are to be kept confidential and never shared
- Students should not share their personal details (address/name/phone number etc.) online
- Students are responsible for any damage (software and hardware) of their own laptop
- Students should never loan their laptop to other individuals
- Students should keep food and beverages away from the laptop since they may cause damage to the device
- Students should use the laptop in ways that are appropriate, meeting RAK Academy expectations and for educational purposes only
- Only laptops are to be brought into the Academy. No mobile phones, tablets or gaming consoles are to be used into school.

Staff use of Mobile Phones:

- Staff should not use mobile phones or other mobile devices for contacting students, young people or their families other than through approved apps installed and configured properly
- Staff should not provide their personal or Academy provided mobile phone number to students, parents, or their families unless properly authorized by the competent authority (as a support hotline or similar preapproved purpose)
- Staff should keep their mobile phones or device switched off or on silent during lessons. They should not interact with these devices during lessons.
- Staff will be issued with an Academy phone where contact with students, parents or guardians is required e.g. on Academy trips
- Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team or if such use is allowed in emergency circumstances
- If members of staff have an educational reason to allow students to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the respective Head of School

Staff use of Personal Devices:

- Currently, there is not a BYOD policy for the staff. Therefore, staff should not bring their laptop or other computing devices to the Academy
- If Staff bring their own laptop or devices into the Academy they will be responsible for any damage or loss (software and hardware) to their laptop or devices
- Staff should not set up and store RAK Academy email accounts on their personal devices and computers. However, they can use web-mail to access their account
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work provided equipment for this purpose
- Staff should not store any Academy related non-public content on their personal devices or on their personal cloud storage accounts (such as Google Drive, One Drive, etc.)
- If a member of staff breaches the Academy policy, a disciplinary action will be taken

Digital images and video:

- We do not identify students in online photographic materials or include the full names of students in the credits of any published Academy produced video materials/DVDs
- If specific student photos (not group photos) are used on the Academy website, in the prospectus or in other high-profile publications, the Academy will obtain individual parental or student permission for its long-term use

Asset disposal:

- Details of all Academy-owned hardware will be recorded in a hardware inventory
- Details of all Academy-owned software will be recorded in a software inventory
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The Academy will only use authorised companies who will supply a written guarantee that this will happen

Appendix 1 – Definitions:

O**nline Child Sexual Abuse:** The online child abuse involves the following:

- Produce self-generated child abuse material
- Engage children in sexual chat
- Arrange an off line meeting for the purpose of sexual activity
- Production, distribution downloading and viewing of child abuse material (child pornography)

Sexting: The act of sending sexually explicit messages or photographs, using mobile phones or other devices.

Sextortion: A form of sexual exploitation where people are extorted with a compromised image of themselves.

Grooming: The premeditated behaviour intended to gain the trust and cooperation of a child prior to engaging in sexual conduct.

Virtual Global Taskforce (VGT): These are specialist law enforcement agencies from around the world working together to fight child abuse online. These include:

- Italy
- New Zealand Police
- United Arab Emirates
- United Kingdom - CEOOP
- United States of America- Department of Homeland Security

Cyberbullying: means bullying through the use of technology or any electronic communication, including, but not limited to a transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted by the use of any electronic device, including, but not limited to a computer, telephone, mobile phone, text messaging device and personal digital assistant. This includes the following:

- Posting slurs or rumours or displaying any defamatory, inaccurate, disparaging, violent abusive, profane, or sexually oriented material about a student on a website or other online application
- Posting misleading or fake photographs or digital video footage of a student on websites or creating fake websites or social networking profiles in the guise of posing as the target
- Impersonating or representing another student through use of that other student's electronic device or account to send e-mail, text messages, instant messages, or phone calls
- Sending e-mail, text messages or leaving voice mail messages that are mean or threatening, or so numerous as to bombard the target's email account, or mobile phone
- Using a camera phone or digital video camera to take and/ or send embarrassing or 'sexting' photographs of other students