ICT and E-safety Policy

Date of Review:	**November 2019**
Approved by:	**Trust Board**
Next Review Date:	**Autumn Term 2020**
Author:	**Director of ICT and Data/Director of HR**

1. Policy Scope

1.1 This policy refers to the on-site internet connection and Rodillian Multi Academy Trust provided ICT devices, systems, and peripherals. These include but are not limited to:

- Fixed computers in offices and classrooms;
- Rodillian Multi Academy Trust provided laptops, tablets and phones;
- Rodillian Multi Academy Trust email systems;
- Remote access solutions to Rodillian Multi Academy Trust networks;
- Rodillian Multi Academy Trust digital cameras, camcorders and audio recorders.

This policy explains the behaviours, which are acceptable and unacceptable with regard to usage of ICT.

1.2 All users should note that ICT systems and internet usage 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.

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

2. Unlawful and Illegal Use

2.1 All material, which depicts the abuse of children and young people, is illegal. Other illegal material includes race hatred and incitement to violence. These are not exclusive categories.

2.2 There may be other information that is deemed to be illegal.

2.3 Accidental access to material, which may be classed as illegal should be reported to the Internet Watch Foundation – www.iwf.org.uk as well as directly to the Head of School.

2.4 **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 Head of School. Once this log has been made the URL if appropriate should be reported to the Internet Watch Foundation – www.iwf.org.uk. 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.

2.5 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 constitutes an illegal offence.** The IWF, is licensed to investigate, you are not. For guidance in this area refer to a member of the leadership team.

2.6 As a user of ICT within the Rodillian Multi Academy Trust 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.

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

2.8 **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.

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

2.10 The storage, distribution, or transmission of unlawful materials could lead to UK authorities alleging criminal liability.

3. Inappropriate Use

3.1 Inappropriate use of the network includes accessing or having possession of material that is thought to be offensive such as, adult pornography of any level, 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 Academy, Local Authority or regional network.

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

3.3 Staff must NOT name their employer on any social networking site, as this could potentially bring The Rodillian Multi Academy Trust 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.

3.4 All communication carried out over Trust ICT systems should be conducted in a professional manner.

4. Violations of system or network security

4.1 Any violations of systems or network security are prohibited, and may result in the user facing criminal and civil action. Violations may include, but are not limited to, the following:

- unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network;
- unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network;
- interfering with any user, host or network including mail bombing, flooding, and deliberate attempts to overload a system and broadcast attacks.

5. Network Usage

5.1 Users must not connect to the network any unprotected machine, insecure devices, or any other devices vulnerable to unauthorised remote access or viruses.

5.2 Users should save work related files, emails and attachments onto the Academy ICT systems, not just onto your personal computers, storage devices, or personal cloud storage areas.

6. Security and Protection

6.1 It is the responsibility of all staff to protect the physical safety, and e-safety of students when using any ICT facilities at The Rodillian Multi Academy Trust.

6.2 All users of the network 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.

6.3 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 including 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.

6.4 You should be aware that it is the responsibility of all staff 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.

7. Email

7.1 The Rodillian Multi Academy Trust, at our sole discretion have the right to access, review, and copy or delete all information contained in emails or otherwise and use it as we consider appropriate.

7.2 Email is not encrypted and therefore is potentially insecure particularly when leaving us 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 secure information transfer.

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

7.4 **Always:**

- assume that whatever you put in an email 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);

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

- remember that emails can constitute/contain personal data under GDPR and should be dealt with in accordance with rules relating to personal data in general (see section 11 for more details).

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

- Any necessary authorised communication with students and parents/carers should be via your academy email account

7.5 **Do not:**

- send abusive, obscene, sexist, racist, 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 our 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);

- 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 our email system for a business purpose unconnected with our business without express permission from a designated senior leader;

- send confidential or sensitive information to persons 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 to correspond in connection with Academy business. Personal email accounts neither provide the audit trail which is necessary nor include the standard disclaimers;

- communicate with students via a personal email account

- give anyone else your passwords.

8. Rules for Computer Use

8.1 The computer systems are owned by The Rodillian Multi Academy Trust and are made available to students to further their education.

- The Trust 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.

- The Rodillian Multi Academy Trust 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 other student's unauthorised use of those facilities or e-mail.

8.2 **Students must abide by the following rules:**

- access to the computers and the internet must only be made via an authorised 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 in the 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 person 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 the Academy 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;

- the 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.

9. Rules for protection of Hardware and Supervision of Student Access

9.1 Protection of Hardware

It is the responsibility of every department 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 are locked.
- When not in use/unsupervised laptop/tablet trolleys are locked in a classroom/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.

9.2 Supervision of Student Access

- Teachers are responsible for the monitoring of student ICT activity in lessons, extra-curricular and extended Academy activities.
- Teachers must remind students of how to use the internet safely and where/how to report any concerns.
- Staff should never use or share personal ICT devices with students, or allow students to use their own personal ICT devices.
- 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 (eg 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 auditable, with clear reasons for the need.

9.3 Good Practice:

- 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.
- Departments/corridors have booking systems.
- Laptops/tablets are returned from the trolley from which they came.
- 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 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.

10. Use of Digital Images and Video

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. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

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 Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Rodillian Multi Academy Trust equipment; the personal equipment of staff should not be used for such purposes.
- 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 Rodillian Multi Academy Trust into disrepute.

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

- Photographs published on the 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 must not use personal devices to share digital images which could be deemed as inappropriate.

11. Data Protection

11.1 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.

11.2 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.

11.3 All staff are expected to complete a short mandatory training programme via our compliance portal. This will cover the basics of GDPR and the individuals responsibility for protecting the personal data the MAT 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.

12. Annex

To support staff and pupils 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.

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.

ICT Usage Policy: Staff

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

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.

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

Always get permission before installing, attempting to install or storing programs of any type on the networked computers.

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

Do not give out the personal information of any staff or pupil from the Multi Academy Trust without the correct authority to do so.

You must ensure that any personal data belonging to students or staff, that you send externally from our organisation or you take offsite is securely encrypted and used appropriately in line with the Trusts GDPR Policy.

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.

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.

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

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

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

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

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.

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

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

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

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

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.

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

Staff must NOT name their employer on any social networking site, as this could potentially bring the Rodillian Multi Academy Trust 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.

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

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

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

Misuse of ICT may lead to disciplinary procedures

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

Name _____ Signature _____ Date _____

ICT Usage Policy: Students

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

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

Do not give out any personal information over the Internet.

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

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

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.

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

Always respect the privacy of other users.

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.

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

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.

Personal computer storage areas and storage disks are not private. ICT support staff may need to view your files to ensure that the system is being used responsibly.

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

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

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

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.

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, 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.