Rise
Flourish & Succeed

Rise Multi Academy Trust: ICT Acceptable Use Policy

(Including Mobile Phones & Cameras)

Rise
Flourish & Succeed

Date of Policy: 3rd September 2025

Approved by the Trust Board: 3rd September 2025

Review Date: September 2027

Signed: 

INTRODUCTION

ICT, or Information and Communication Technology, refers to the diverse range of technologies, tools, and resources used to process, store, manage, transmit, and exchange information in a digital form. It encompasses both hardware (like computers and telecommunications equipment) and software, including applications, networks, the internet, and systems that enable communication and information sharing.

ICT is provided to support and improve the teaching and learning in the Trust as well as ensuring the smooth operation of our administrative and financial systems.

This policy sets out our expectations in relation to the use of any computer or other electronic device on our network, including how ICT should be used and accessed within the Trust.

The policy links to the Rise Information Security policy and Rise Information Security Protocols document which provides advice and guidance to our employees on the safe use of social media. The acceptable use of ICT will be covered during induction and ongoing training will be provided, as appropriate.

This policy does not form part of any employee's contract of employment and may be amended at any time. However, any breach of this policy is likely to result in disciplinary action.

SCOPE AND PURPOSE

This policy applies to all employees, governors, volunteers, visitors and any contractors using our ICT facilities. Ensuring ICT is used correctly and properly, and that inappropriate use is avoided is the responsibility of every employee. If you are unsure about any matter or issue relating to this policy you should speak to your line manager, the network manager or a senior member of staff.

The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT to protect the Trust and its employees from risk.

Employees may be required to remove internet postings that are considered a breach of this policy. Failure to comply with such a request may itself result in disciplinary action.

Any failure to comply with this policy may be managed through the disciplinary procedure.

If you reasonably believe that a colleague has breached this policy, you should report it without delay to your line manager or a senior member of staff.

MONITORING

The contents of our ICT resources and communications systems are our property. Therefore, employees should have no expectations of privacy in any message, file, data, document, social media post, blog, conversation, or any other type of information or communication transmitted to, received from, stored or recorded on our electronic information and communications systems. Do not use our ICT resources and communications systems for any personal matter that you wish to be kept private or confidential.

We reserve the right to monitor, intercept, and review employee activities using our ICT resources and communication systems, to ensure that our policies are followed, data is protected, and systems are used only for legitimate business purposes. Monitoring may include checking for compliance with security updates and identifying potentially malicious activity.

We may store copies of data or communications accessed as part of monitoring for a period of time after they are created, and in doing so will comply with GDPR.

POLICY RULES

In using the Trust's ICT resources, the following rules should be adhered to. For advice and guidance on these rules and how to ensure compliance with them, you should contact the network manager or a senior manager.

The network and appropriate use of equipment:

- You are permitted to adjust computer settings for comfort and ease of use.
- Computer hardware has been provided for use by employees and pupils and is located in designated areas. If there is a problem with any equipment or if you believe it would be better positioned elsewhere to support your work, please contact your line manager.
- Do not disclose your login username and password to anyone under any circumstances. You must not use any shared credentials.
- You are required to change your password regularly, in line with system prompts or Trust notifications. All passwords must be strong (using a mix of uppercase and lowercase letters, numbers, and symbols) and unique to each account. Do not write passwords down or store them in locations where they could be accessed by others.
- Do not allow pupils to access or use your personal login credentials for any system. Pupils are not permitted to use staff access rights, as this could lead to a breach of GDPR and compromise network security. Allowing pupils such access could put you at risk if your accounts are used.
- Before leaving a computer unattended, you must lock the screen or log off the network. You must ensure the device is secured to prevent unauthorised access or misuse.
- Ensure projectors linked to the network are switched off when not in use.
- Only software provided by the network may be run on Rise computers and laptops. You are not permitted to import or download applications or games from the internet unless Advanced IT and your line manager agree to do this.
- You must not use any removable storage devices (RSDs), such as USB pens or external hard drives.
- Pupil or staff data, or any other confidential information should not be stored on a memory stick and should only be stored on encrypted devices and not taken off the premises unless it has been encrypted to ensure data protection and confidentiality.
- Removable storage devices should only be used for Trust purposes, outside of our premises if they are encrypted or have appropriate password protection in place.

MOBILE DEVICES, LAPTOPS & CAMERAS

The following rules are for use of any laptop, electronic tablets, mobile phone or other mobile device including those provided by the Trust. Referred to as mobile device(s):

- If you choose to use your own mobile device for school/Trust business, you do so at your own risk and must ensure compliance with this policy and the GDPR policy if using any data or network.
- Access to our wireless network must be approved by the network manager (Advanced IT) or Headteacher.
- You must ensure that any mobile device is protected by a strong password or PIN, and, where available, encryption and remote wipe capability must be enabled. This is essential if you are taking the mobile device off our premises.
- You must never leave your mobile device in an unsecured place, for example in your car.

- Any personally owned mobile devices must have up to date anti-virus and security updates installed before connecting to the network. They must also comply with Trust security requirements, including encryption and approved security settings.
- You must ensure you have the appropriate permissions and security in place in order to access our network at home.

To ensure the safety and welfare of the children in our care this policy outlines the protocol for the use of personal mobile phones and cameras in the school.

- All staff must ensure that their mobile phones, personal cameras and recording devices are stored securely during working hours on school premises or while on outings. This requirement also applies to visitors, Relish staff, contractors, volunteers and students.
- Mobile phones or smart watches must not be used in any teaching area in school or within toilet or changing areas.
- Only school equipment should be used to record classroom activities. Photos should be uploaded to the school system as soon as possible and must not be sent to or stored on personal devices.
- During school outings nominated staff will have access to a school mobile which can be used for emergencies or contact purposes.
- All telephone contact with parents or carers must be made using the school phone, and a note of the conversation should be recorded on CPOMS.
- Parents or carers are permitted to take photographs of their own children during a school production or event. The school protocol requires that photos of other people's children are not published on social networking sites such as Facebook.
- Photographs may only be taken and used for any purpose if consent has been given and consent must be in the form of a completed consent form. If using Arbor MIS for consent, you must ensure that the log is kept proving consent has been obtained and given by the parent/guardian.
- It is essential that photographs are taken and stored appropriately to safeguard the children in our care.
- Only designated devices provided by the Trust are to be used to take any photos of children.
- Images taken on the designated camera(s) must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
- All staff are responsible for the security of the cameras when assigned.
- Images taken and stored on the camera must be downloaded in school as soon as possible, ideally once a week by IT.
- Under no circumstances must cameras of any kind be taken into the toilet area whilst students are or may be present.
- No personal device must ever be used to photograph children.

INTERNET SAFETY

- Never give out personal information such as your address, telephone number or mobile number over the internet without being sure that the receiver is from a reputable source.
- Never give out personal information about a pupil or another employee over the internet without being sure that the request is valid, and you have the permission to do so. Always check if you are asked for information that this does not constitute a subject access request (SAR).

- Always alert our IT provider AIT (help@advanceditservices.co.uk) or Headteacher if you view content that makes you feel uncomfortable or you think is unsuitable. Remember that any personal accounts accessed on our network will be subject to monitoring.
- Report any suspected phishing emails, malware warnings, or security breaches immediately.
- Always alert our It provider AIT (help@advanceditservices.co.uk) or Headteacher if you receive any messages that make you feel uncomfortable or you think is unsuitable.

INTERNET AND EMAIL

- The internet and email facilities are provided to support the aims and objectives of the Trust. Both should be used with care and responsibility.
- Use of the internet at work must not interfere with the efficient performance of your role. We reserve the right to remove internet access to any employee at work.
- You must only access those services you have been given permission to use.
- Before sending an email, you should check it carefully and consider whether the content is appropriate. Treat emails like you would any other form of formal written communication. Take extra care when forwarding emails that include prior correspondence.
- Although the email system is provided for business purposes, we understand that employees may on occasion need to send or receive personal emails using their work email address. Remember these will be subject to the monitoring section of this policy.
- This should be kept to a minimum and must not interfere with your ability to carry out your role effectively. When sending personal emails from your work email account you should show the same care in terms of content as when sending work-related emails.
- The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be considered under the disciplinary procedure.
- You should not send electronic messages which are impolite, use obscene language, are indecent, abusive, discriminating, racist, homophobic or in any way intended to make the recipient feel uncomfortable. This will be considered under the disciplinary procedure.
- If you receive an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, you should not forward it to any other address, but you should alert the Head Teacher or your line manager.
- Do not access any sites which may contain inappropriate material or facilities, including but not limited to:
- *Proxy*
- *Dating*
- *Hacking software*
- *Pornographic content*
- *Malicious content*
- *Music downloads*
- *Non-educational games*
- *Gambling*
- Do not send malicious or inappropriate pictures of children or young people including pupils, or any pornographic images through any email facility. If you are involved in these activities the matter will be referred to the LADO and the police.
- Under no circumstances should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or young people. This material includes, but is not limited to pornography, unethical or illegal requests, racism, sexism, homophobia, inappropriate language, or any use which may be likely to cause offence. If you are not sure about this or come across any such materials you must inform the Head Teacher or a senior manager.

- Do not upload or download unauthorised software and attempt to run on a networked computer, in particular hacking software, encryption and virus software.
- Do not use the computer network to gain unauthorised access to any other computer network.
- Do not attempt to spread viruses.
- Do not transmit material subject to copyright or which is protected by trade secret which is forbidden by law.
- Never open attachments or click links in emails if you are unsure of their origin; delete these messages or report them immediately to the network manager or senior manager. Be particularly cautious of unexpected requests to share personal or financial information.
- Do not download, use or upload any material from the internet, unless you have the owner's permission.

The following acts are prohibited in relation to the use of the ICT systems and will not be tolerated:

- Violating copyright laws
- Attempting to harm minors in any way
- Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity
- Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service
- Uploading, posting, messaging or otherwise transmitting any content that without the right to transmit under any law or under contractual or fiduciary relationships (such as
- inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements)
- Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party
- Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.
- "Stalking" or otherwise harassing any user or employee
- Collection or storage of personal data about other users

If you are in any doubt about this policy in practice, please speak to your line manager or the Head Teacher before acting.

REVIEW OF POLICY

This policy is reviewed as required by the Trust in consultation with the recognised trade unions. This ensures transparency, fairness and smoother implementation.

We will monitor the application and outcomes of this policy to ensure it is working effectively and remains aligned with the Department of Education's digital and technology standards. Updates will be made as required to reflect changes in guidance and legislation.

EMPLOYEE AGREEMENT

ICT Acceptable Use Policy	
Employee (print name):	
Employee Agreement: • I have read and understood the Trust's ICT acceptable use policy. • I will use the computer network, internet and other technologies in a responsible way in accordance with the rules set out in the policy. • I understand that network and internet access will be monitored. • I understand my obligations in relation to use of social media and portable devices.	
Signed:	**Date:**

To be handed back to the school office.

Scan or place signed form in employee's personnel file