Media Trust IT and Digital Security Policy

Date of Policy	September 2024
Review Frequency	Biennially
Date of next Review	September 2026

Purpose

The purpose of this policy is to set out the parameters on how staff should use the technology and systems that Media Trust provides you with to do your job. This policy applies to all Media Trust staff. This policy covers computers, internet access, remote access connections, file storage, phones, and webmail. Media Trust reserves the right to monitor the use of communications, IT, and digital devices to ensure the compliance of the policy, to monitor whether its use is legitimate, to assist in the investigation of alleged wrongdoing, to comply with any legal obligation, and to access records in case of business needs (such as absence due to sickness).

Employees are reminded that the same protocols and security need to be applied when working from home or any remote location.

Line managers and in turn Heads of Departments are responsible for ensuring their staff members understand the policy and are complying with it.

This policy works in conjunction with the Data Protection Policy and other Media Trust policies. Employees are reminded to ensure they have read and understood these policies also. It does not form part of any employee's contract of employment and may be amended at any time.

Communication tools and use of our systems

Communication needs to be professional and courteous and must not contain illegal, abusive, obscene, pornographic, derogatory, defamatory, or discriminatory content. Employees are reminded that in all communications, written and verbal, they are representing Media Trust.

You should not: send, forward, or read private emails at work which you would not want a third party to read; send or forward chain mail, junk mail, cartoons, jokes or gossip; contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to others who do not have a real need to receive them; or send messages from another person's email address (unless authorised) or under an assumed name.

Do not use your own personal email account to send or receive emails for the purposes of our business. Only use the email account we have provided for you.

No personal data is to be sent either in the body of an email or as an attachment on email, or other communication tools. The transfer of such information should be via links from our cloud storage systems. If the recipient is unable to receive it in this manner, this needs to be password protected as an attachment and the password communicated separately through a different platform or using a one-time password.

Many platforms are now available for communication, and we often find ourselves using multiple platforms and tools. Our recommendation is to use Microsoft Outlook for external communication and Microsoft Teams for internal communications. When using alternative platforms, users are reminded to ensure they are adhering to our policies.

Employees are reminded that communication tools, such as email, are not storage systems for data. Any relevant data is to be transferred into our cloud storage in the relevant location to ensure the relevant persons have access and no excess data is stored within communication tools. Employees are reminded to regularly clear and delete from all folders on their email system and ensure that the deleted items folder cleared on a weekly basis.

Using AI tools at Media Trust

Incorporating AI into the workplace brings significant benefits but also poses new risks. AI systems must be used responsibly to prevent unauthorised access or misuse of personal/sensitive data. Employees should follow Media Trust's AI guidelines document, which outlines ethical use and data privacy measures. These guidelines ensure AI tools are used responsibly, safeguard against cyber threats, and optimise productivity across teams.

Distribution list protocols

Distribution emails should be sent through Salesforce.

Equipment

Any devices that are used to access company resources must be registered with the company portal to ensure correct security protocol are adhered to.

No data should be stored on desktops or download folders, all data is to be kept in the relevant folders on our cloud storage system (SharePoint).

Computers and software should be shut down at the end of each working day in order that updates can be installed. Individuals are responsible for regularly checking that the OS system on their machine is up to date.

Screen savers should be activated, and machines locked when stepping away in an office or at home. If in a public place, your equipment must not be left unsupervised.

Passwords

Password Safes must be used for both the generation and storage of passwords and the master password needs to meet the requirements of LastPass or equivalent.

Passwords for machines need to be a minimum of 8 characters long and include upper and lower case and at least one number and one symbol. These require changing every six months.

Where passwords are needed to be shared, they should match with the above criteria and only shared with those that need them via a one-time password. When anyone with access to these shared passwords leaves Media Trust, these passwords must be changed.

If any member of staff becomes aware or is suspicious of their password being compromised, they should immediately contact the COO, or in the case that the COO is unavailable, a member of the Senior Management Team.

Working in public places

You may want to on occasion work from a public space such as a café, train, or a Media Trust partner's offices. If this is the case, you will need to consider the following:

- The space is suitable for you to work – do you have a suitable chair, is the screen and keyboard at the correct height?

- Is the space private – can your screen be overlooked, are you able to take and make calls? If not, you will need to consider what work you are able to complete and how.
- Is the internet connection secure and password protected
- If you need access to company data, this should be done through our cloud storage.
- No printing of personal information should be done without the express permission of the COO or CEO.

Internet access

We expect all employees to use the Internet responsibly and for work related purposes. Staff are permitted to use IT equipment for personal use (for example, accessing webmail or online shopping at lunchtimes), but are reminded that they should not be using work time to do this. Employees should adhere to all protocols and all other policies whilst doing so, as well as ensuring it should not be used to access any webpage or download any image or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral, or which in any way could bring Media Trust into disrepute.

Software

The Managed Software Centre is on every machine and will allow for the auto deployment of software updates, provided users close relevant programmes. Optional pre-approved software is available to download from the software centre. Any other software requiring download will require permission of the COO and admin password.

Data security

Salesforce should be the centralised point for all data and not duplicated elsewhere. Employees are reminded that accessing data on any of our systems that is not relevant to your job is prohibited.

You must not delete, destroy, or modify existing systems, programmes, information, or data (except as authorised in the proper performance of your duties).

You must not download or install software from external sources without authorisation from the COO. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from the COO.

Any known, accidental, or suspected data breach must be reported to the COO immediately, or in the case that the COO is unavailable, a member of the Senior Management Team.

If staff observe their email behaving oddly (due to rules being set up to hide hacking behaviour) or other unusual computer behaviour, do not email but call the COO immediately to alert to this possibility. Turn off the machine and disconnect from the network. We encourage over vigilance and ask staff to report anything outside of what might be considered normal.

Barracuda

Check and appropriately mark Barracuda emails when received to ensure the best possible email security. The options are Deliver, Allow List and Block List. If you are unsure you can select Deliver so you can see more detail but ensure once review the appropriate option is then selected i.e. Allow List and Block List.

Add emails to block list if spam is received and not picked up by Barracuda. If any addresses are being blocked that need to be received, notify the COO who will add them to the whitelist. Should you receive any emails that are not picked up by Barracuda that look suspicious please do not email but call the COO.

Training

Training is available to any staff that are unable to use any of the Media Trust systems. It is the responsibility of the employee to inform their line manager of any issues they have with the use of any systems.

All staff are required to complete

- **Describe basic cybersecurity threats, attacks, and mitigations** – this 20-minute course focuses on what Cybersecurity is, the threat landscape and basic mitigation strategies
- **Securing you: Basics and beyond** – this is a 30-minute course which focuses on identifying common threats and how to protect yourself against them

Important: Once you've completed the training, the completion page allows you to share the achievement. Please share with the digital team so they can log and verify you've completed it.

Misuse of IT facilities

Failure to adhere to our IT and Digital Security Policy can result in disciplinary proceedings up to and including dismissal. Examples of this includes:

- Misuse of the Internet or our communication systems.
- Creating, viewing, accessing, transmitting, or downloading pornographic, offensive, obscene, or discriminatory material.
- Disclosing without permission confidential information about us, our business, our staff, or any of our service-users.
- Attempting to discover a user's password.
- Using the computer systems to act abusively.
- Attempting to circumvent the network's security.
- Knowingly running and installing programmes intended to damage the computer systems.
- Deliberately wasting computer resources.
- Leaving laptops unattended in a public place.