NMAT ACCEPTABLE INFORMATION TECHNOLOGY USE POLICY (Non-statutory)

NUNTHORPE MULTI ACADEMY TRUST

Preamble

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of the Trust's programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Acceptable Use policy governs the use of the Trust's corporate network that individuals use on a daily basis in order to carry out business functions.

This policy should be read in conjunction with the other policies in NMAT's Information Governance policy framework.

Scope

All policies in the Trust's Information Governance policy framework apply to all Trust employees, any authorised agents working on behalf of the Trust and/or academies within the Trust, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

General Principles

All must use our information technology and communications facilities sensibly, professionally, lawfully, consistently with their duties and in accordance with this policy and other NMAT expectations and procedures.

At all times employees must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information.

Every NMAT employee will be given access to the intranet and/or internet as appropriate to their job needs. For those who do not have daily PC access occasional access will be arranged, as necessary, by the IT Team.

All PC/network access will be secured through usernames and passwords, and no individual is permitted onto the system using another employee's username and/or password. Employees are not permitted to share their username and/or password with anyone inside or outside the Trust. Individuals will be allowed to set their own passwords, and must change them as frequently as requested by the system set-up requirements.

NMAT ACCEPTABLE INFORMATION TECHNOLOGY USE POLICY (Non-statutory)

All information relating to our staff/students and the Trust and individual Academy's operations are confidential. All must treat our paper-based and electronic information with utmost care.

Many aspects of communication are protected by intellectual property rights which can be infringed in a number of ways. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

Particular care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind a person and/or the Trust and can be produced in court in the same way as other kinds of written statements.

The Trust may remain liable for employee's email activity and social media activity if this is an academy/Trust account and as such any offensive, explicit or indecent email content is expressly prohibited and the sending of such content will lead to disciplinary action.

Employees should ensure emails do not contain defamatory or inaccurate content, in line with appropriate legislation such as:

- Freedom of Information Act 2000
- Equality Act 2010
- Human Rights Act 1998
- The General Data Protection Regulations 2016/679
- Employment Rights Act 1996
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Public Interest Disclosure Act 1998
- Part Time Workers (prevention of less favourable treatment) regulations 2000

Although disclaimers are on external emails, the requirement to act responsibility and appropriately remains the responsibility of the employee.

If an employee has any concerns with the contents of an external email, they should report it immediately to their academy's IT Network Manager.

Internet and Email use for personal purposes
Although our Internet and e-mail facilities are provided for the purposes of allowing the Academies to operationally function, we accept that staff may occasionally want to use them for your own personal purposes.

Employees may access the Internet and their personal email accounts during their breaks and lunch times. This is permitted on condition that all the procedures and rules set out in this policy, and the other relevant policies, are complied with.

Unauthorised use of email and Internet
NMAT will not tolerate use of email and internet for inappropriate purposes, including:

- any messages that could constitute bullying, harassment or other detriment;
- on-line gambling;
- accessing or transmitting pornography;
- accessing other offensive, obscene or otherwise unacceptable material;
- transmitting copyright information and/or any software available to the user;

- posting confidential information about other employees, NMAT or its students or parents.

Downloading of material
In order to prevent the introduction of virus contamination into the software system the following must be observed:

- unauthorised software including public domain software, magazine cover disks/CDs or Internet downloads must not be used, and
- all software must be virus checked by the IT team before being used.

On-line blogs
It is not permitted for employees to contribute to on-line blogs during working hours, or using a computer belonging to the Trust. The following rules apply:

- personal blogs should contain a disclaimer that the views expressed on it are personal views of the author only;
- All should not at any time make comments in a blog which bring the Trust or academy into disrepute;
- All should not reveal confidential NMAT information, or information on staff/students/parents/governors etc;
- All should not at any time make comments in a blog which amount to bullying, harassment or any other detriment towards other employees/ staff/students/parents/governors or any other individual working in connection with Trust.

Storage of emails
Employees should ensure they regularly audit their emails in order to archive or delete those that contain information that is no longer required in order for the Trust to comply with its legal obligations under the GDPR.

Company's website
Unless the employee is responsible for the upkeep of the NMAT or an Academy's website as part of their role, they are not permitted to add anything to the website without express permission of the Head of School/Executive Principal and the IT Network Manager.

Monitoring
The Trust is ultimately responsible for all business communications but subject to that will so far as possible and appropriate, respect your privacy and autonomy. NMAT may monitor all employee's business communications for business reasons.

Enforcement
Failure to comply with this policy may result in disciplinary action being taken against an individual. If there is anything in this policy that a person does not understand, please discuss it with their line manager, the IT Network Manager and/or HR team.

Social networking websites and blogs
Social networks are web-based communication structures that enable easy communication and relationship building between individuals via the Internet, many of which include additional access to further methods of interaction, such as email and instant messaging. While the Trust considers the widespread use of social networking applications an effective and useful method for communication in the appropriate context, the potential for misuse by workers, during and out of work hours, is such that the following guidelines are in place.

NMAT ACCEPTABLE INFORMATION TECHNOLOGY USE POLICY (Non-statutory)

NUNTHORPE MULTI ACADEMY TRUST

Purpose
This social networking procedure has the following purpose:

- to help protect the Trust against potential liability;
- to give employees clear guidance on what can and cannot be said about NMAT and/or its academies or other workers;
- to help workers separate their professional and personal communication;
- to comply with the law on discrimination, data protection and protecting the health of employees;
- to be clear about the use of monitoring within NMAT academies.

Process
Access to email and the Internet is provided during working hours for the purpose of effectively completing work and use must comply with all NMAT/Academy policies and procedures.

The Trust will not tolerate employees using social networking sites for unofficial or inappropriate uses. Specifically:

- All should not at any time upload photographs to your social networking sites of themselves or any other employee taken in a work situation or in a work uniform. No defamatory comments about NMAT and/or its Academies should be made on such sites at any time;
- All should not at any time include information that identifies any other employee/student/parent/Governor/Trustee/Member or any other individual working in connection with the Trust;
- All should not at any time express opinions on such sites which purport to be the opinion of the Trust or one of its Academies, nor comments representing the employee's own views on NMAT;
- Any personal blogs should contain a disclaimer that the views expressed on it are personal views of the author only;
- All should not at any time make comments on such sites which bring the Trust into disrepute;
- All should not reveal confidential NMAT information, or information on employees/student/parent/Governor/Trustee/Member or any other individual working in connection with the Trust.
- All should not at any time make comments on such sites which amount to bullying, harassment or any other detriment towards other employees/student/parent/Governor/Trustee/Member or any other individual working in connection with the Trust.

The term "use" includes accessing social media by means of PC, mobile phone or by any other device.

Monitoring
It is recommended that all employees use strict privacy settings on their social network profiles. NMAT monitors employee's internet and work email usage regularly and may undertake more in depth monitoring where considered necessary. This includes monitoring the websites employees visit and any other matters referred to in this policy.

Enforcement
Any employee who the Trust suspects has breached this policy will be subject to the Trust's disciplinary procedure.

Breaching copyright laws.
Copyright laws cover information posted online. Employees must not breach copyright laws by copying information from the Internet without permission.

NMAT ACCEPTABLE INFORMATION TECHNOLOGY USE POLICY (Non-statutory)

Social media policy
The Trust operates a social media policy to govern the use of this media within NMAT. The policy covers profile pages and other resources maintained by employees on networking sites including, but not limited to, Facebook, Twitter and LinkedIn, as well as blogs, forums, message boards, review sites and online polls.

This policy sets out how employees must behave when using the NMAT's social media platforms and governs how employees should refer to, and promote NMAT academies on their own personal accounts.

Policy aims
This policy applies to all employees, contractors and volunteers who use social media either for personal or professional reasons. It is important that employees using social media in the workplace use it in a way which does not adversely affect NMAT's reputation.

Social media can involve communication between job applicants and employees and is an avenue for NMAT to promote and control their reputation. Social media may blur the boundaries between what is home and work. Access is often public, even amongst a limited group of connected accounts, and comments are often permanent.

Employees should be honest and respectful when using social media. Everything posted on social media may be tracked back to the source so employees must ensure content posted on social media accounts, both in a work and personal capacity, fits with NMAT's ethos.

Terms of use
Social media usage for work purposes is controlled by the IT Network Manager.

When using social media, either in a personal or work capacity, during or outside working hours, posts on social media must not:

- compromise NMAT, disclose confidential data or disclose sensitive data;
- must not damage NMAT's reputation or brand;
- must not breach copyright or data protection;
- contain libel or defamatory content;
- must not engage in bullying or harassment;
- be of illegal, sexual or offensive content;
- interfere with your work commitments;
- use the name of NMAT and/or its academies to promote products or political opinions.

Social media content attributable to you which breaches the terms of this policy, or the other related policies, may result in an investigation and disciplinary action under NMAT's disciplinary policy.

Social media and recruitment
Recruitment processes are increasingly utilising social media as a method of engaging job-seekers. Due to the increasing amount of content posted online, viewing candidate's social media profiles is a quick and effective way of checking details contained in a CV or getting an idea of the personality of the candidate.

NMAT permits reviewing the social media profiles of candidates for recruitment purposes. This review must be carried out in accordance with NMAT's policies and code of conduct. Before accessing a candidate's social media profile, permission must be sought from the NMAT HR and Compliance Lead

and/or the Executive Principal. Permissions will only be given once the reasons for access and the benefits it will bring to the process, which cannot be found elsewhere.

Accessing of the candidate's profile page may be disclosed to the candidate during the recruitment process. Where information is discovered that makes the candidate unsuitable for the position, the candidate will be notified and they will be entitled to make representations about the information and their unsuitability.

NMAT reserves the right to check the social media accounts of employees in accordance with the internet and monitoring policy.

Using electronic devices during work hours
NMAT provides certain employees with electronic devices and this section governs their usage, along with any use of personal devices at work. Trust owned electronic devices should be kept in good condition by employees. The device should remain charged and connected to the network (as far as coverage permits) during working hours. Employees may only use NMAT devices in line with the monitoring, internet and social media policies.

Guidelines on the use of NMAT electronic devices
The following guidelines apply:

- NMAT devices may only be used for authorised business use;
- Personal use is not permitted, except where employees have been given prior approval from their line manager;
- Employees may not install or download any extra apps on to an NMAT electronic device;
- Employees should not open any file attachments on an NMAT device which have been received from unknown sources;
- Confidential or sensitive NMAT data contained on a NMAT device must be appropriately protected and secured;
- Use may be monitored under NMAT's monitoring policy;
- Any communication sent from an NMAT device must comply with accepted conventions and standard practice for business use;
- NMAT devices must not be used to display or access offensive, explicit, pornographic or racist material.

Loss or damage
Employees are responsible for the safekeeping of their NMAT electronic device. Employees should keep their NMAT device safe and try to avoid loss or damage. Any loss or damage caused by the employee's negligence will result in a charge for the repair or replacement. NMAT reserves the right to make a deduction from an employee's next salary payment for the cost of repairs or replacement.

NMAT electronic devices should be secured with a password or PIN and kept out of sight. NMAT devices must not be left in a vehicle.

Reasonable precautions should be taken by employees to limit the risk of their NMAT electronic device being stolen. If it is stolen, employees should inform the IT Network Manager, the Head of School and the NMAT HR and Compliance Lead immediately.

NMAT ACCEPTABLE INFORMATION TECHNOLOGY USE POLICY (Non-statutory)

Return of equipment
Employees may be requested to return their NMAT electronic device at any time. Employees must return their device upon termination of their employment. Whenever returned, the NMAT device must be accompanied by any additional accessories that were also issued to the employee. NMAT reserves the right to make a deduction from an employee's final salary payment of the cost of the replacement of the tablet and/or any missing accessories, if any of these are missing or damaged.

Breach of this procedure
NMAT reserves the right to remove an NMAT electronic device from an employee should any terms of this policy be breached. NMAT may also take disciplinary action. Inappropriate use of an NMAT device may be treated as gross misconduct and could result in summary termination of employment.

Bring your own device (BYOD) to work procedure
The intention of the Bring Your Own Device procedure, (BYOD), is to ensure the security and integrity of any NMAT data which may be stored on these devices. Any user that requires to use BYOD (any device brought on site either connected or not) should understand the Trust retains the right to seize and check the device if there is reason to believe it is not being used in accordance with the AUP or this policy.

Principles
NMAT recognise that certain advancements in technology will improve effectiveness and aid productivity within an Academy and across the Trust, therefore authorised employees will be permitted to bring their personal devices to work. NMAT must ensure the correct usage of these devices and have, therefore, created this procedure to set certain standards of behaviour. Employees must read and agree to the terms of this policy prior to the use of any personal device for Academy or Trust purposes. The Trust reserves the right to revoke the procedure or the use of personal devices should it be found that an employee is in breach of this procedure.

Employee responsibilities
Any access to the Trust's network must be approved by the academy's IT Network Manager.

- The device must only be used during working time for any work related activities that directly or indirectly impact or support the education of NMAT students and/or NMAT business activities;
- Illicit materials should not be stored or transmitted from any personal device.

Devices and security

- Any personal device will be checked by the IT Department to ensure appropriate configuration to allow access to the academy's infrastructure. Any device that has not been approved by the I.T. Department will not be permitted access – This includes USB and other external drives;
- Any personal device must contain a level of security in line with our existing IT infrastructure, this must include passcode protection and automatic locking when idle;
- Any personal device that has not been checked and approved for use by a member of the IT team will be unable to connect to the Academy's network.
- Access to NMAT's infrastructure will be in line with current security levels and user profiles;
- Any NMAT data and confidential information available on a personal device should be accessed by the authorised user only and this should be in line with the existing policies. No access to the device or NMAT's network will be permitted for third party users;
- Reasonable steps will be taken by NMAT to ensure employees private personal data will be protected fully and not be retained in any way unless it directly involves Academy activity.

Furthermore, it is the employee's responsibility to ensure that all devices and personal data is backed up in the event that this data is lost and the device wiped;

- If an employee's personal mobile device is lost or stolen you must advise the IT Network Manager, the Head of School and the NMAT HR and Compliance Lead immediately in order to ensure access to the NMAT's network is deactivated;
- The responsibility for the upkeep of the device and any liability or risks associated with the use of the device for business purposes remain with the employee;
- The personal device should be made available for monitoring upon request by the IT Network Manager and/or Head of School. Every effort will be taken to ensure that personal data is not accessed on the device, however in the event that this is not possible no records of the information will be stored and that data will not be used unless required by law;
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of NMAT and personal data due to operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

General

- Personal devices remain the responsibility of the employee and all associated costs for the device and the running of the device shall remain with the employee;
- NMAT accepts no responsibility for any loss or damage to personal devices that are the result of employee failure to observe rules, procedures or instruction, or, as a result of your negligent behaviour;
- Misuse of NMAT information, data and/or software provided by the NMAT could be treated a gross misconduct which could result in formal disciplinary action being taken up to and including dismissal;
- Upon termination of employment you must ensure that all NMAT data and software is removed from your device on your last day of work at the latest. Evidence of this must be presented to the IT department, who may require you to submit your device to them for inspection and removal of NMAT data and software if necessary;
- Any breach of this procedure may result in formal disciplinary action being taken up to and including dismissal.

Breach of this procedure

Failure to adhere to this procedure may be viewed as a breach of the NMAT's disciplinary rules and will be dealt with under NMAT's disciplinary procedure.

Use of NMAT mobile phones

Only certain job roles require the provision of an NMAT mobile phone. Where provided, they are for NMAT business use only.

Employees should ensure they keep the NMAT mobile phone in good working order. The mobile phone should remain charged and connected to the network (as far as coverage permits) during working hours so business calls can be received as necessary. The cost of line rental and normal business call usage will be covered by NMAT.

Loss or damage

Employees are responsible for the safekeeping of their NMAT mobile phone. Employees should keep their NMAT mobile phone safe and try to avoid damage or loss. Any loss or damage caused by the employee's negligence will result in a charge for the repair or replacement. NMAT reserves the right to make a deduction from an employee's next salary payment for the cost of repairs or replacement.

NMAT ACCEPTABLE INFORMATION TECHNOLOGY USE POLICY (Non-statutory)

NMAT mobile phones should be secured with a password or PIN and kept out of sight. NMAT mobile phones must not be left in a vehicle. Reasonable precautions should be taken by employees to limit the risk of their NMAT mobile phone being stolen. If it is stolen, employees should inform the Executive Principal and the NMAT HR and Compliance Lead immediately.

Return of equipment

Employees may be requested to return their NMAT mobile phone at any time. Employees must return their device upon termination of their employment. Whenever returned, the NMAT mobile phone must be accompanied by any additional accessories that were also issued to the employee. NMAT reserves the right to make a deduction from an employee's final salary payment of the cost of the replacement of the phone and/or any missing accessories, if any of these are missing or damaged.