DIOCESE OF SOUTHWELL
& NOTTINGHAM
MULTI ACADEMY TRUST

SNMAT

IT Acceptable Use Policy

Policy:	ICT Policy
Approved by:	Board of Directors
Date:	November 2024
Review Cycle:	Annual

Versions:

VERSION	**DATE**	**AUTHOR**	**CHANGES**
2020	MAR 2020	DO – Trust IT Director	Initial version.
2020.1	MAR 2020	DO	Several minor amendments throughout the policy are highlighted in yellow. Amendment to wording of sentence in rationale: "The Trust monitors emails for compliance in respect of financial and personal medical information which, if sent by e-mail, could breach GDPR legislation. Such e-mails are prevented from being sent." Addition to policy on page 9 (setting up social media accounts), highlighted in yellow. Addition to policy on page 14 in the staff/volunteer acceptable use agreement, highlighted in yellow. A number of sentences have been removed throughout the policy.
2021	MAR 2021	JSAV	The 2020 policy has been reviewed by the IT Director and no changes or additions are required. The Board will be asked to approve as is.
2022	MAY 2022	MY – Trust IT Lead	Paragraphs numbered throughout the policy. No other changes required.
2023	NOV 2023	MH – Trust IT Manager	Renamed IT Acceptable Use Policy to reflect contents and modern terminology. Updated layout and font use. Various changes throughout to recognise that previous policy is superseded in many areas by the SNMAT eSafeguarding and Cyber Security policies. Network Manager and roles adjusted to reflect SNMAT job descriptions. Updated SNMAT IT Team responsibilities to reflect adherence to existing policies. Amended Third Party IT Provision

			responsibilities to include legislation and KCSIE.
2024	May 2024	MJH – Trust IT Manager	Full revision. Reflect that implementation is covered in other policies such as eSafeguarding, Cyber Security and Artificial Intelligence. Removed signed consent forms in favour of statement that IT Acceptable Use Policies will be displayed either on first use of IT devices, before sign-in, or upon sign-in of cloud devices. Removed signed forms in favour of statement that any use of IT equipment and enrolment in an academy means automatic assumption of acceptance of the IT Acceptable Use Policy. Added that acceptance of this policy is obligatory when using any SNMAT IT device.

EXECUTIVE SUMMARY

This policy outlines the obligations on the part of Diocese of Southwell and Nottingham Multi-Academy Trust (SNMAT), its academies, and other stakeholders regarding the acceptable use of SNMAT owned Information Technology (IT) devices and the steps the Trust and its academies take to ensure good practise and compliance with cyber and data security and safeguarding obligations.

RATIONALE

IT is an essential resource in education. IT helps support learning and learning, as well as playing an important role in the everyday lives of children, young people, and adults alike. Consequently, academies have an obligation to educate members of the SNMAT community with

SCOPE

The aim of this policy is to:

- Provide direction and guidance in the safe use of IT.
- Ensure users of SNMAT IT are aware of their legal obligations when using IT.
- Encourage consistent and professional practice in the use of IT.
- Ensure that all users are clear about their responsibilities in using IT.
- Advise users of SNMAT IT on monitoring arrangements.

This policy applies to:

- All members of the SNMAT community, including staff, students, pupils, parents and carers, volunteers

The policy also applies to those affiliated by third parties who work in Trust Academies and Trust Teams.

LINKS WITH OTHER POLICIES

The IT Acceptable Use Policy must be read, understood and agreed in conjunction with other policies:

- GDPR and Data Protection Policy
- Artificial Intelligence (AI) Policy
- Bring Your Own Device (BYOD) Policy
- eSafeguarding Policy
- Social Media Policy
- Cyber Security Policy
- Smart and Mobile Technology Policy

ROLES AND RESPONSIBILITIES

BOARD OF DIRECTORS

The Board of Directors are accountable for the compliance of Trust and Academy devices, infrastructure and stakeholders to Cyber Security, eSafeguarding, and acceptable use of IT within an academy context.

LOCAL GOVERNING BODIES

The responsibility for ensuring that academy IT networks comply with the relevant IT policies has been delegated to Local Governing Bodies. They must approve an IT Acceptable Use Policy that meets the needs of their specific academy.

THE PRINCIPAL/HEADTEACHER

The Principal/Headteacher is responsible for ensuring that all users understand the conditions under which academy IT services may be used, and the expectations of this policy around good practise and professional behaviour. They must:

1. Shape and approve an IT Acceptable Use Policy that meets the needs of their academy.
2. Ensure all staff and pupils read and understand the policy.
3. Ensure that all staff and pupils receive regular guidance and suitable training if necessary to enable them to adhere to the IT Acceptable Use policy.

DESIGNATED SAFEGUARDING LEAD AND SENIOR LEADER RESPONSIBLE FOR DIGITAL TECHNOLOGY

The Senior Leadership Team Digital Lead and Designated Safeguarding Lead must:

1. Ensure that their academy IT Acceptable Use Policy meets the needs of the Academy eSafeguarding Policy.

STAFF

Are responsible for:

1. Reading and complying with other policies linked here; for example, GDPR, eSafeguarding and AI.
2. Ensuring that they have read, understood and follow their academy IT Acceptable Use Policy.
3. Enusring that all pupils and students adhere to the academy IT Acceptable Use Policy, and provide guidance and direction if required for them to be able to adhere to expectations.

PARENTS AND CARERS:

Are responsible for:

1. Ensuring that they have read, understood their academy IT Acceptable Use Policy.
2. Enusring that their children adhere to the academy IT Acceptable Use Policy, and provide guidance and direction if required for them to be able to adhere to expectations.
3. Encourage their children to adopt the safe use of the internet and digital technologies at home and should inform the relevant academy if they have concerns over online safety.

PUPILS AND STUDENTS

Pupils and students should:

1. Ensuring that they have read, understood and follow their academy IT Acceptable Use Policy.

TRUST IT SUPPORT TEAMS

Are responsible for:

1. Ensuring technical policies are in place to support the acceptable use of IT; network, systems and services security, data protection and encryption, eSafeguarding, passwords, filtering and monitoring, communications and more.

2. Ensuring that users are presented with their academy IT acceptable use policy where possible, when first using devices.

OBLIGATIONS

- You are expected to comply fully with this policy. SNMAT and its Academies reserve the right to take disciplinary action if it considers that you are acting in contravention of this policy.

- With any use of SNMAT IT equipment, it is deemed that you have accepted the obligations of this policy and agreed to the terms laid out in the user agreements.

- Student use of IT, Microsoft 365 and Google G-Suite services is a mandatory part of their teaching and learning, and thus consent and acceptance of this policy is assumed for any children enrolled in one of our academies.

- If you are in any doubt about whether your proposed use of SNMAT equipment or systems is in accordance with this policy, then you should seek guidance from the Trust IT Manager, relevant Academy IT staff or Head Teacher before undertaking the activity.

- When using SNMAT IT, you remain subject to the same laws and regulations as the physical world. It is expected that your conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

IT ACCEPTABLE USE

USER ACCOUNTS

- All SNMAT users are provided with a username/email address and password. Staff passwords will have to be changed periodically to adhere to eSafeguarding and Cyber Security Policies.

- Staff are encouraged to Combine three random words to create a password that’s ‘long enough and strong enough’ ((for example *applenemobiro*)). Passwords generated from three random words is a good way to create unique passwords that are ‘long enough' and ‘strong enough’ for most purposes, but which can also be remembered much more easily.

- You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any Academy account.

- Passwords must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

- You must only use your own login and password when logging into IT systems. Passwords must be changed whenever there is a system prompt to do so or where there is a possibility that there could otherwise be a possible compromise of the system. Passwords should not be re-used or recycled across different systems.

- Where temporary passwords are issued to any individual, for any reason, then they should be changed at first logon to a permanent password.

EMAIL ACCOUNTS

- Users granted a SNMAT a professional email account ial to them being able to carry out their professional duties properly and fully. SNMAT email accounts are for academy related communications and all SNMAT related communications must be conducted via acdemy accounts only. SNMMAT systems are suitably protected and are the secure and authorised means of conducting work related correspondence.

- All communications made via SNMAT email accounts must relate to academy duties and be of a tone and nature which reflects your professional role and the nature of the communication in question. The degree of care and professionalism should be the same as that applied with a written letter.

- Email is not the preferred form of communication for confidential, personal or other sensitive information (e.g. any comments relating to job performance or disciplinary issues). Email cannot be regarded as purely private, only to be seen by the receiver.

- Email should be managed, XXXXX

- All online activity, both in the academy and outside the academy, must not bring the individual, in their professional role or WNAT into disrepute.

- Authorised ICT staff may access your professional email account if you are absent and there is WNAT related business captured within the account which cannot be otherwise accessed and which requires action before your anticipated return.

USING THE INTERNET

- SNMATs internet web filtering policy has been developed to help our schools maximise the safety of our students as they use the internet, whilst at the same time retaining the flexibility needed for effective teaching and learning.

- Staff are responsible for following eSafeguarding guidelines for use of the internet in advance of learning taking place.

- You must not browse, download, upload or distribute any material that could be considered discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous or defamatory. You must always adhere to the SNMAT eSafeguarding and Social Media Policies.

- Parents are encouraged to adopt the safe use of the internet and digital technologies at home.

MICROSOFT 365

- SNMAT provisions Microsoft 365 services, email, Teams, OneDrive and SharePoint and other tools.

- These tools should be used to collaboratively create, edit and share files for school related projects and communicate via email with members of staff.

- These services are entirely online and available 24/7 from any Internet-connected devices.
- Staff, Students and Pupils must refer to, and adhere to the SNMAT eSafeguarding Policy for the use of Microsoft 365 services.

IT DEVICES

- SNMAT IT devices are provided to enable you to fulfil your professional and educational duties.

- You are responsible for all activity carried out on SNMAT systems, whether accessed via SNMAT or personal devices. You should not allow any unauthorised person to use WNAT ICT facilities.

- You may not plug personal ICT hardware into WNAT equipment without specific permission from the relevant member of ICT staff.

- You must not access, load, store, post or send from WNAT equipment or via a professional email any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to WNAT or may bring WNAT into disrepute.

- Use of WNAT equipment, systems and networks, should be undertaken in compliance with the Data Protection Act 2018, Computer Misuse Act 1990 and the Copyright, Designs and Patents Act 1998. In the event that you have any concerns as to whether the intended use is duly compatible with relevant legislation, then you should seek advice from the relevant ICT staff prior to undertaking the activity.

- You must not do anything to jeopardise the integrity of the IT Infrastructure, without prior approval for example;

1. Damaging, reconfiguring or moving equipment.
2. Unless with prior approval of the ICT Manager installing software
3. Reconfiguring or connecting equipment to the network
4. Installing services or servers onto the network
5. Deliberately or recklessly introducing malware

PHISHING, MALWARE AND VIRUSES

- Malware and viruses are malicious software that cause considerable harm to IT devices and networks. You are required to take all steps to void the introduction of viruses or malware onto any SNMAT IT device or network, including, but not limited to:

- Ensure that any file downloaded from the internet is from a legitimate source. Avoid use freeware,

- Do not use removable media, unless encrypted with prior permission from authorised IT staff. Use your SNMAT and Academy provided OneDrive or SharePoint storage where possible to access files in school and at home.

- Do not open any email that you are not expecting, especially any that contains an attachment.

- Do not open links to questionnaires, offers, requests from unknown sources.

- Delete emails with attachments that you were not expecting even if you know the person sending, if the wording seems "odd" in some way. These programs can often spoof the Sender field in emails to make it look like someone you know is emailing you.

- Do not attempt to install hardware or software. Contact your relevant IT Support Team.

- Do not interrupt any updates or anti-virus scanning that is taking place on devices.

- Report any attempted phishing e-mail to the ICT Manager in order that they can make sure that investigations can be made into potential other users receiving the email. Often a phishing e-mail is sent to a number of people. See 12.2 below.

- Read and understand the SNMAT Cyber Security Policy, Appendix 1 on how to recognise a cyber-attack and what action to take.

LANDLINE AND MOBILE PHONES

- All telephones provided are for work related calls.

- Phone calls to international and premium rate numbers are unacceptable at all times, unless specifically required for your professional duties.

- Mobile telephones should be secured with a suitable biometric, PIN or passcode security.

- The use of 3CX mobile phone app on personal devices.

SAFE USE OF IMAGES

Images of pupils and/or individuals may only be taken, stored and used for professional purposes in accordance with the law and in accordance with SNMAT Safeguarding, Data Protection, eSafeguarding and GDPR policies. In any event particular regard must be given to the provision of written consent of the parent, carer or individual to the taking, storage and use of the images. Parents are encouraged to adopt the safe use of the internet and digital technologies at home.

PERSONAL AND CONFIDENTAL DATA

- All use of personal and confidential data must be in accordance with the Data Protection Act 2018.

- This applies equally, whether on WNAT premises, taken off WNAT premises or accessed remotely.

- You must ensure that personal data is kept secure and is used appropriately.

- To protect personal, sensitive, confidential or classified data and prevent unauthorised access to it, this will include, but may not be limited to:

- Ensure screen displays of such data are, at all times, kept out of direct view of any individual who does not need to access that information as part of their professional role and out of direct view of any third parties;

- Ensure screens are locked before moving away from the computer, at any time;

- Ensure logoff from ICT equipment is fully completed when you are going to be away from it for a longer period of time.

- In the event that you consider that you need to take personal data out of WNAT premises or access it remotely then appropriate authorisation should be sought in advance. Personal or sensitive data taken off site must be encrypted and particular care must be taken when travelling by public transport both to ensure personal data is not inadvertently viewed and to ensure that it is not left behind.

USING SNMAT OWNED DEVICES AT HOME

- You may be supplied with SNMAT equipment to utilise at home and outside of your usual workplace setting. This includes laptops, tablets, mobile phones or other internet-enabled devices. Such equipment must be treated and used in the same way as it would be in the workplace. You are expected to abide by this policy when using all such SNMAT devices.

- On request you must make SNMAT owned device available for antivirus updates and software installations, patches or upgrades.

- You must not make copies of any SNMAT software or licences for use outside the organisation or outside the rules prescribed by the software's license.

- All data must be saved into SNMAT Microsoft 365 services, either OneDrive or SharePoint and not locally or elsewhere on a device.

- Personal data must not be stored on SNMAT devices.

- You are responsible for ensuring that all equipment is stored and kept safely and securely. Any protective equipment must be utilised properly.

- On termination of employment, resignation or transfer, you must return all SNMAT owned equipment to your Line Manager.

- In normal circumstances you should not be using personal equipment for work purposes.

- As detailed above in the section on Personal and Confidential Data, ICT equipment must never be left unattended in an area accessed by the public and/or when travelling. When travelling by car, if you have to leave the car unattended then ICT equipment should be kept locked in the boot and out of sight where it is not possible for you to take the equipment with you.

- WNAT reserves the right to inspect all equipment utilised at home. The Trust retains the right to verify equipment for audit purposes at any time throughout the duration of its use. Staff are therefore obliged to produce any equipment within a reasonable timeframe (5 working days) where requested to assist with this verification process.

- All staff should refer to and adhere to the SNMAT GDPR Policy for protection of data.

SOCIAL MEDIA

Social media tools are excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with users and the wider community. Whilst social media tools can provide tremendous benefits to schools, they also have serious security risks in their use.

Personal use of social media, personal websites, blogs, etc. should make no reference to SNMAT, its pupils, or colleagues regardless of whether these sites are accessed while at work or not. Any derogatory comment which expressly or impliedly criticises WNAT, it's employees, pupils or a relevant third party may be cause for disciplinary action (in addition to any claim for defamation).

Staff, Parents and Carers should refer to, and adhere to the SNMAT Social Media Policy for responsible use of Social Media.

ARTIFICIAL INTELLIGENCE

SNMAT recognises the positive impact that using Artificial Intelligence (AI) in an education setting can bring, especially in reducing workload and supporting pupils with educational needs. However, we are committed to ensuring compliance with guidelines on data protection, plagiarism and exam malpractice to maintain safeguarding and academic integrity.

AI offers an incredible opportunity to transform the way that we teach and learn, and empowers educators and students to personalise their learning, produce smart content, automate tasks and deliver better engagement.

Staff, students and pupils should refer to, and adhere to the SNMAT Artificial Intelligence Policy for responsible use of AI.

DISPOSAL OF IT EQUIPMENT

SNMAT and its Academies will dispose of all redundant ICT equipment in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and the Data Protection Act 2018 (DPA). Any equipment that is to be resold must have a demonstrable audit trail to prove that is has been disposed of in line with ESFA requirements and authorisation has been sought by the same, where appropriate.

INCIDENT REPORTING

You should report any actual security breaches or attempted security breach, loss of equipment or data, to the Data Protection Officer (DPO).

Concerns regarding virus, phishing emails, unsolicited emails, any unauthorised use or suspected misuse of IT or any of matter of concern, should be reported to your Designated Safeguarding Lead in the event of a safeguarding issue, or your IT Support Team.

If you receive an email, through your professional email account, either from within SNMAT or from any third party that you consider to be abusive then that should immediately be reported to the relevant Line Manager.

All users should take reasonable precautions to protect their passwords. If a user thinks that their username or password has been used without their permission, they must change the password and inform the Principal/Headteacher as soon as practically possible. The Principal/Headteacher should ensure that new users are issued with appropriate usernames and passwords. When a user leaves their job, whether leaving the school or not, the head teacher should ensure that all usernames and passwords for that user are suspended as appropriate.

Parents are encouraged to adopt the safe use of the internet and digital technologies at home and should inform the relevant academy if they have concerns over online safety.

MONITORING

When using SNMAT IT, you remain subject to the same laws and regulations as the physical world. It is expected that your conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

All monitoring, surveillance or investigative activities may be conducted only by authorised SNMAT staff. This must be done in accordance with the following policies, legislation or regulations:

- SNMAT eSafeguarding Policy
- DfE Keeping Children Safe in Education Statutory Guidance (2024)
- The Data Protection Act 2018;
- The Human Rights Act 1998;
- The Regulation of Investigatory Powers Act 2000 (RIPA)8
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2009.

Testing, Monitoring and Reporting is clearly defined in the SNMAT eSafeguarding Policy.

Staff/Volunteer Acceptable Use Agreement

I understand that I must use academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school (as per the BYOD policy and in line with GDPR best practices).
- I understand that the academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the academy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school / academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the academy's social media and other policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy and the MAT have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school / academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment (see BYOD policy). I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. I will not use personal email addresses on the academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs).

- I will check the recipient(s) of any email I send carefully to ensure that it is not received by any inappropriate individuals either in or outside of the organisation.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy / MAT Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school / academy:

- I understand that this Acceptable Use Agreement applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.