SAMWORTH CHURCH ACADEMY

DIOCESE OF SOUTHWELL & NOTTINGHAM MULTI ACADEMY TRUST

ICT Policy

Approved by the MAT Board of Directors - 24 March 2020

Policy:	ICT Policy
Approved by:	SNMAT Board of Directors
Date:	09 March 2020
Review cycle:	Annual

VERSION CONTROL			
VERSION	DATE	AUTHOR	CHANGES
2020	March 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.

ICT POLICY

Introduction

Information and Communication technologies are an essential resource in academies. They help to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, academies need to build in the use of these technologies in order to arm children and young people with the skills to access life-long learning and employment.

Currently children and young people in academies use these technologies both inside and outside of the classroom for:

- Accessing websites
- Email and instant messaging
- Chat rooms and social networking
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading
- Gaming
- Mobile/smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst these technologies are exciting and in the main, beneficial both in and out of the classroom, all academies need to be aware of the range of risks associated with the use of these technologies.

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures as well as on good user education and training.

Scope

The aim of this policy is:

To provide direction and guidance in the use of ICT;
To encourage consistent and professional practice in the use of ICT;
To protect the Trust, the academy and users from inappropriate usage, security risks and legal liability;
To ensure that all users are clear about their responsibilities in using ICT;
To advise users on the monitoring arrangements for the usage of ICT.

This policy applies to:

All permanent, temporary and casual staff working at a school;
Pupils/students;
Consultants, contractors, agency staff, governors, parents, volunteers and others working at the school, including those affiliated with third parties who may be given access to ICT services.
(Note: throughout this policy, the word “user” is used to cover all of the above).

Rationale

ICT use in an academy setting should be legally regulated, this includes the content of email, or sites downloaded from the Internet; privacy issues, monitoring of communications and surveillance at work and employment relations. Further legal advice should be sought, if appropriate, from the Trust HR advisors or the Legal Quickline.

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.

Roles and Responsibilities

Board of Directors

The Board of Directors is ultimately accountable for ensuring that the trust/academy infrastructure/network is as safe and secure as is reasonably possible and the acceptable use of ICT in all of the academies in SNMAT.

Local Governing Bodies

The responsibility for ensuring that the academy ICT infrastructure/network is as safe and secure as is reasonably possible. They must approve an Acceptable Use of ICT Policy to meet the needs of their specific academy has been delegated to the Local Governing Bodies.

The Principal/Headteacher

The Principal/Headteacher is responsible for ensuring that the ICT infrastructure/network is as safe and secure as is reasonably possible on a day to day basis and the implementation of the academy's Acceptable ICT Use Policy to ensure all adults and children understand the conditions under which academies ICT services may be used.

Staff

The staff are responsible for:

- ensuring that they have read, understand and follow the academy's Acceptable Use of ICT policy;
- ensuring they comply with GDPR guidelines;
- ensuring that pupils/students follow the Acceptable Use of ICT Policy for Pupils/Students in class.

The Network Manager/Technical Staff/ICT Support Service

The Network Manager/Technical Staff/ICT Support Service is responsible for ensuring:

- that the academy's technical infrastructure is as far as is possible within the school's financial and organisational constraints, secure as well as monitored for misuse and malicious attack (Appendix 1);
- that the academy meets required online safety technical requirements and any Trust ICT Policy that may apply (Appendix 1);
- that procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups, are in place and secured;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed as necessary;
- that web filtering is applied and updated on a regular basis and that its maintenance is not the sole responsibility of any single person;

- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- that the use of the network/internet/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal/Headteacher for investigation/action/sanction;
- that monitoring software/systems are implemented and updated as agreed in academy policies.

Objectives

It is the policy of the Trust/academy to:

- ensure that all 'users' use e-mail and the internet in an acceptable manner, in accordance with e-mail and internet codes of practice for schools and the academy's acceptable use of ICT Policy (Appendix 2);
- ensure that ICT is used securely by putting both the necessary technical safeguards in place and establishing and enforcing policies and procedures for the academy's use of ICT in line with GDPR principles;
- monitor the use of ICT as appropriate to ensure that the SNMAT policies and procedures are being complied with.

Links with Other Policies

The ICT Policy must be read in conjunction with the other following policies:

Bring Your Own Device (BYOD) Policy
Data Protection Policy
Social Media Policy
Policy for Child Protection to Safeguard the Welfare of Children
E-Safety Policy

Guidance for Implementation

This guidance applies to the safe use of ICT equipment and services provided by an academy in SNMAT. Anyone discovering a breach of this guidance, or who is in receipt of electronic communication that appears to contravene the guidance described below, should raise the issue with the principal/head teacher in the first instance.

Technical Infrastructure/Equipment

The academy should ensure that the following security measures are in place in relation to the ICT infrastructure:

- that the academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented;
- that academy technical systems are managed in ways that ensure that the academy meets recommended technical requirements outlined in relevant body policy and guidance;
- that there are regular reviews and audits of the safety and security of academy technical systems;
- that servers, wireless systems and cabling are securely located and physical access restricted;
- that software licences are checked for compliance to ensure the academy does not breach the Copyright, Designs and Patents Act 1988 or the Intellectual Property Act 2014;

- that an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person;
- that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data;
- that these security measures are tested regularly;
- that the academy infrastructure and individual workstations are protected by up to date anti-virus software;
- that an agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the academy systems;
- that an agreed policy is in place regarding the extent of personal use that users (staff/students /pupils/community users) and their family members are allowed on academy devices that may be used out of the academy;

If the academy has a managed ICT service provided by an outside contractor, it should ensure that:

- the managed service provider is fully aware of the Trust E- Safety Policy, ICT technical requirements and related IT policies.
- the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the academy.

Appropriate and Inappropriate Usage for ICT

Terms used:

Appropriate: activities listed are acceptable in terms of ICT use.
Inappropriate: activities listed as inappropriate may potentially lead to misconduct and disciplinary proceedings. In some cases, this could lead to dismissal and legal action.

Passwords

The academy should ensure that:

- all users have clearly defined access rights to academy technical systems and devices;
- all users (at KS2 and above) are provided with a username and secure password which is disabled when the user leaves the institution;
- users are responsible for the security of their username and password and are required to change their password as required.
- group or class log-ons and passwords are provided for KS1 and below, where requested by the academy but that staff are made aware of the associated risks;
- the "master/administrator" passwords for the academy ICT system, used by the Network Manager (or other person) is also be available to the Principal/Headteacher or other nominated senior leader and kept in a secure place (e.g. school / academy safe);

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.

Appropriate:	Inappropriate:
• Users only using their own account to carry out day to day work; • Users not disclosing their password to allow others to access their account. Users should be aware passwords are for the benefit of the academy and are the proprietary and confidential information of the academy; • Users selecting a password that is easy to remember but not for others to guess; • Users not selecting obvious passwords, such as the name of a close relative, friend or pet; • Compliance with the password policy for each computer system.	• Requesting passwords personally assigned to other users; • Using a session via another users' password; • Sharing passwords with other users.

Use of E-Mail or Internet

The Internet provides users with access to worldwide information services, bringing new opportunities for communication. However, this also brings with it risks to pupil safety and all staff must ensure they have read and understand the E-Safety policy

Internet filtering must be in place according to the academy's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the academy's Leadership Team and Governors. The academy should ensure that:

- illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list;
- content lists are regularly updated and internet use is logged and regularly monitored and that there is a clear process in place to deal with requests for filtering changes;
- internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet;
- IT has provided enhanced/differentiated user-level filtering allowing different filtering levels for different ages/stages and different groups of users – staff/ pupils/students etc;

Staff should be aware that websites, search results etc., may be safe and appropriate one day but unsafe a day later. All members of the academy community should be aware that filtering software is not always effective and cannot always be relied on (in isolation) to safeguard children and young people;

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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.

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. Risks such as people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and exploit children. Reference must be made to the Social Media Policy before setting up and using such sites. It should be noted that official SNMAT email details must be used to create these social media accounts and it is highly recommended that the credentials of these accounts be lodged with the central MAT team, both when created and when login details are changed.

Use of PCs, Laptops, Servers, i-pads, mobile phones and Other Hardware

The academy should ensure that:

- an agreed policy is in place that allows forbids staff from downloading executable files and installing programmes on trust/academy devices unless specifically authorised to do so;
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs / DVDs) by users on trust/academy devices.

Appropriate:	Inappropriate:
• Storing school data; • Loading text, images, video or audio streams about day to day work activities; • Storing limited amounts of personal data (where agreed by the principal/head teacher).	• Loading unauthorised or untested software; • Allowing unauthorised users to access laptops used away from school; • Failure to keep laptops used away from school secure; • Storing confidential or personal data or information on removable media without adequate protection or encryption; • Deliberate, reckless or negligent introduction of viruses; • Storing personal material protected by copyright which has not been purchased; • Loading files containing pornographic, offensive or obscene material.

ICT tools provided by the academy should always be used (e.g. work provided digital cameras, memory cards, laptops etc.,) rather than personally owned equipment unless the academy has authorised the use of personal devices under the Bring Your Own Device Policy (BYOD).

Monitoring the Use of Electronic Communications

The contents of Trust's IT resources and communications systems are the property of the Trust. Although the Trust/academy aims not to intrude into the private lives of staff or students, it reserves the right to monitor the use of academy computers, video and audio machines, phones and fax machines, social media posts, e-mail conversations or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems to safeguard pupils/students, ensure policies and

procedures are being complied with and for legitimate business purposes. Users should be made aware of this in the Acceptable Use Policy. Appropriate records of any monitoring will be kept, which can be accessed on request to the Principal/Headteacher (or the senior member of staff authorised by the Principal/ Headteacher).

Review

This policy is reviewed annually by the Trust in consultation with the recognised trade unions. The application and outcomes of this policy will be monitored to ensure it is working effectively.

Appendices - Model Acceptable Use Forms

Parent/Carer Permission Form

Use of Cloud Systems Permission Form

Staff Acceptable Use Agreement

Use of ICT Parent / Carer Permission Form

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: .....

Date: .....

Use of Cloud Systems Permission Form

Office 365 for Education services – requires a school to obtain 'verifiable parental consent' for their children to be able to use these services.

The school uses Office 365 for Education for *pupils / students* and staff. This permission form describes the tools and pupil / student responsibilities for using these services.

The following services are available to each *pupil / student* and hosted by Microsoft as part of the school's online presence in Office 365:

Mail - an individual email account for academy use managed by the academy

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs – The Microsoft Office suite of on-line office productivity tools including Word, Excel, Powerpoint, OneNote (inc for classroom) and Teams

Using these tools, *pupils / students* 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 computer. Examples of student use include showcasing class projects, building an electronic portfolio of academy learning experiences, and working in small groups on presentations to share with others.

The academy believes that use of the tools significantly adds to your child's educational experience.

As part of the Microsoft terms and conditions, we are required to seek your permission for your child to have an Office 365 for Education account:

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent / carer of the above student / pupil, I agree to my child using the school using Office 365 for Education.	Yes / No

Signed: .....

Date: .....

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.

Staff / Volunteer Name: .....
Signed: .....
Date: .....