



DIOCESE OF
ST ALBANS
MULTI-ACADEMY TRUST

Trust Policy

ICT Acceptable Use Policy

Policy type	Trust wide (Tier 1)
Renewed	Every 3 years
Author/Responsible Officer	Chief Operating Officer and Partnership Education
Approved by	Trust Board
Date of ratification	April 2025
Date of next review	April 2028

This policy is a mandatory policy for all DSAMAT Academies and must be implemented without any amendments

Enabling all to flourish: Rooted in God's love



Our mission, vision and values

The Trust has a clear **mission** at its core, ensuring that all pupils are enabled to flourish, rooted in God's Love - academically, socially, spiritually, physically and mentally. This is central to our work and rooted in our Christian foundation (John 10 v 10). Our commitment to mutual flourishing within the school community is built upon our shared belief in Church of England principles. In our Trust, just as in the wider Church of England community, 'flourish' refers to prospering, thriving and growing – not shrinking out and dying. It means prayerfully encouraging all within our schools so that they might prove fruitful, successful and contented in the longer term. We seek to provide space generously for all to flourish in life and all of its structures. Equal treatment for all pupils, staff and the wider community is a core part of enabling this long term, holistic flourishing.

We have a clear **vision** about creating successful schools for the benefit of their communities. All schools provide rich and diverse curricula which evolve to meet the needs of their children and local communities, as well as delivering educational excellence to enable them to continue to flourish in later life.

The way we work and deliver against our mission is critical to our Trust. We have shared, agreed **values** of:

Hope; Nurture; Equality; Respect; Collaboration

The Trust's vision is underpinned by a Christian values framework which is adopted by all schools. It provides clear expectations for all Trust employees on how we wish our values to impact on all areas of school life. It draws on, and is informed by, the National Church of England Vision for Education and the Diocesan Board of Education Vision.

Each school within the Trust has a personalised vision for education, developed locally to reflect the individual character and needs of the school community. This vision is underpinned by the Trust's wider vision, and agreed with the Trust, but it is owned and driven by the headteacher and their LGB.

Our community

The Trust are dedicated to delivering education that serves local communities. Our schools are inclusive, welcoming those from all and no faiths, from all abilities and backgrounds. We believe in providing a high-quality education, underpinned by Christian values, which enables every child to flourish.

Underpinning all of the Trust's work is a belief in educational excellence. The Trust serves all stakeholders by providing schools with the highest levels of academic rigour and pastoral care.

Our schools are places where children and young people develop and thrive intellectually, socially, culturally and spiritually. All of the Trust's schools teach a broad and balanced curriculum within national guidelines focusing on core skills. This is designed to ensure that all pupils reach their academic potential and seek to enrich their experience along the way. Pupils will be enabled to succeed in an atmosphere of high expectation, aspiring to educational excellence with a firm foundation of values.

Enabling all to flourish: Rooted in God's love



This policy forms part of our Trust governance and ensures that we are held to the highest standards as we carry out our duties.

Statement of Intent

This is the Diocese of St Albans Multi-Academy Trust (DSAMAT) over-arching ICT Acceptable Use policy and must be implemented and adhered to in each of the academies within the Diocese of St Albans Multi Academy Trust along with those working within the central team.

This policy will be implemented and adhered to from the first day of any academy joining the Trust. For the remainder of this document, the Diocese of St Albans Multi Academy Trust will be referred to as DSAMAT.



Contents:

- 1. Introduction**
- 2. Data Protection**
- 3. Cyber Threats**
- 4. Account Security**
- 5. Pupil Protection**
- 6. Reporting of Incidents**
- 7. Conduct**
- 8. Use of School IT Systems**
- 9. Respect of School Resources**
- 10. Use of Social Networking and Online Forums**
- 11. Portable Electronic Devices and Laptops**
- 12. Law**
- 13. Monitoring and Review**



1. Introduction

- 1.1 Technology is continually evolving and becoming more integral in professional use, including in schools and academies. The internet is a powerful technology, and we try to provide as much freedom as possible in terms of its use. All users should always remain safe when accessing the internet and other digital mediums.
- 1.2 All members of staff, governors and volunteers using ICT equipment within DSAMAT must ensure that they abide by the ICT Acceptable Use Policy.
- 1.3 This policy is intended to ensure that:
- Staff, governors and volunteers are responsible users and remain safe when using the internet and other communications technologies for educational, personal and recreational use
 - The school computer systems and their users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
 - Staff are protected from the potential risk in their use of technology in their everyday work
 - The school will endeavour to ensure that staff and volunteers will have good access to digital technology and mediums to improve their work, and the learning opportunities for pupils' education. In return, staff, governors and volunteers are expected to agree to be responsible users
- 1.4 All members of staff, governors and volunteers have a responsibility to use the Trust's ICT equipment in a professional, lawful, and ethical manner, consistent with the Trust's ethos, national and local guidance and expectations, the law, and relevant Trust and school policies including:
- Code of Conduct
 - Data Protection
 - Safeguarding / Keeping Children Safe in Education
 - E-Safety (including social media)
 - Cybersecurity
- 1.5 This policy should be read in conjunction with the ICT Acceptable Use Policy for pupils. Those principles apply equally in this policy.

2. Data Protection

All staff, governors and volunteers need to adhere to the below:

- I understand that I must not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the IT infrastructure of the school
- I understand that I must use my work login account to access any of the ICT systems
- I understand that I must not allow anyone to use my work login for any of the ICT systems for any reason and I understand that I must take every reasonable precaution to secure any data or equipment that I remove from the school's premises
- I understand that equipment removed from site will be my personal responsibility and I am advised to check that its loss or damage is covered by my personal insurance. Where

Enabling all to flourish: Rooted in God's love



this is not covered, I understand that it will be covered by DSAMAT's insurance through the RPA.

- I understand that the Trust can and will monitor any data on the network to ensure policy compliance, and to aid in resolving network issues as efficiently as possible
- I understand the importance of protecting sensitive data such as pupil data by not leaving information available and unattended on any device, whether on or off Trust premises
- I understand that any IT systems provided by the Trust are primarily intended for educational use and that any use, professional or recreational, will be within the policies set by the Trust
- I understand that any personal data of pupils, staff or parents & carers must be kept in accordance with the Data Protection Act 1988/2018 and GDPR Regulations 2016.
 - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely.
 - Any personal data which is being removed from the school site will be encrypted by the use of an encrypted memory stick or work cloud-based system. I must take all reasonable precautions to encrypt the data during use and to securely delete or destroy the data once it is no longer required.

3. Cyber Threats

One of the most common cyber threats are phishing attacks. These will be carefully crafted emails to mislead you into entering private credentials, such as your username and password. Once this information has been entered, the strength of the password will be irrelevant and it will allow criminals access to your email and files, and potentially those of others. If you receive an unexpected email or an email that you don't believe is genuine, please follow the below steps:

1. Ensure that no links in the E-Mail are clicked
2. Forward the E-Mail to support@partnership.education (this will raise a ticket on the Helpdesk and the email content can be scanned to confirm it's genuine)
3. If you believe it is malicious delete it from your inbox
4. If the email is deemed malicious and the sender is not genuine the email address will be added to the blocked senders list to prevent future emails
5. If for any reason you do click a link / enter your credentials, please contact the IT Helpdesk immediately so that additional security measures can be implemented asap. The faster the issue is raised the greater chance of preventing malicious activity

4. Account Security

- You are responsible for keeping your login details safe.
- You must not share your password with anyone, including friends or family.
- Passwords must be complex. This means:
 - At least 8 characters long

Enabling all to flourish: Rooted in God's love



- Include both upper- and lower-case letters
- Include numbers
- Include at least one special character (e.g., !, @, #, \$)
- Do not use obvious passwords like your name, the word “password”, or “123456”.
- If you think someone else knows your password, report it and change it immediately.

5. Pupil Protection

All staff, governors and volunteers must adhere to the below:

- I understand that pupils must be supervised at all times when in an ICT suite
- I understand my role regarding acceptable use and my role in enforcing it
- I will escalate non-compliance by members of staff, volunteers or pupils in accordance with Trust procedures
- I understand that I have a duty to remind pupils of appropriate use of internet technologies on a regular basis
- I understand that I should guide pupils in their exploration of the internet
- I understand that I should promote the idea of pupils “thinking before they click” in an effort to reduce any incidents of inappropriate material being viewed and make pupils aware of what they should do in the event of seeing inappropriate material
- I understand misuse by pupils should be sanctioned by your school E-Safety and Safeguarding procedures and where necessary, escalated to the appropriate person(s).

6. Reporting of Incidents

All staff, governors and volunteers will report immediately any or all of the following to Partnership Education via support@partnership.education:

- Any websites accessible from within the Trust which I feel are unsuitable in any way for student access
- Any abuse of any ICT system(s), software or hardware, providing name(s) and location(s) where available
- Any inappropriate content suspected to be on any ICT system. This extends to, but is not limited to, email, documents and pictures.
- Any breaches, or attempted breaches, in security

7. Conduct

All staff, governors and volunteers need to adhere to the below:

- At all times, I will conduct myself professionally during computer usage. This includes being polite and using the system in a safe, legal and appropriate manner. Among uses that are considered unacceptable are the following:
 - Using, transmitting or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist or defamatory language or materials
 - Making ethnic, sexual-preference or gender-related slurs or jokes



- I will respect, and not attempt to bypass, security or access restrictions in place on the computer system
- I will not access, copy, remove or otherwise alter any other user's files without their express permission
- I will respect copyright and ensure I do not use any information breaching copyright law. Where work is protected by copyright, I will not download or distribute copies (including music and videos). I will not take copies of music CDs or videos and place them on the Trust's IT systems, unless the appropriate licenses have been purchased to make such copies
- When I use any personal handheld / external devices (laptops, mobile phones, USB devices or tablet devices) on the Trust's IT infrastructure, I will follow the rules set out in this agreement, in the same way as if I was using the school's equipment. I will follow any additional rules set by the Trust pertaining to such use. I will not connect any personal equipment directly to the network infrastructure
- I will not retain any images on personal equipment. Where these images are published and can be seen outside of the Trust's firewall, such as on the individual school's website and/or VLE, it will not be possible to identify by name or other personal information, those who are featured.
- I understand that it is not acceptable to use my personal email account to communicate with pupils
- I will ensure that when I publish any material which includes photographs of pupils or colleagues, I have ensured that their written permission has been sought before they are used

8. Use of School IT Systems

All staff, governors and volunteers need to adhere to the below:

- I will not open any attachments to emails where the source is not known and cannot be trusted, due to the risk of the attachment containing viruses or harmful software
- I will not 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 use any programs or software that might allow me to bypass the filtering or security systems in place to prevent access to such materials
- I will not disclose or share any personal information about any student or employee to anyone outside of the Trust. Exceptions will include the Police and social services as outlined in the individual school's Data Protection policy
- I understand that data transferred outside of the Trust's secure network, must be encrypted if sent by email

9. Respect of School Resources

All staff, governors and volunteers need to adhere to the below:

- I will not (without permission) try to make large downloads (greater than 500mb) or uploads that might take up internet capacity and prevent other users from being able to carry out their work

Enabling all to flourish: Rooted in God's love



- I will not take up internet capacity by continuous streaming of live radio or live video over the internet, which has the effect of preventing others from being able to carry out their work effectively
- 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. I understand that all software is installed by Partnership Education and any plans for new software should be discussed with them before any purchase is considered
- I will not add any hardware to the system, including laptops, printers or scanners
- I will not disable or cause any damage to Trust equipment belonging to others
- I will endeavour to use the resources in an economical way and use the appropriate equipment wherever possible
- I will ensure that I do not waste resources by printing multiple copies to printers and use photocopiers instead
- I will check my email on a regular basis and clear messages so that my mailbox does not become full

10. Use of Social Networking and Online Forums

All staff, governors and volunteers need to adhere to the below:

- I will take care when using social networking websites such as Facebook or X, even when using social networks in my own time using personal equipment. Social Networking sites can invite users to participate in an informal manner that can leave you open to abuse, and often do not discern between adult users and children
- I will not allow any pupil to access personal information I post on a social networking site
- I will not under any circumstances have current pupils as “friends” on any social media site. It is also strongly advised that staff do not have any former pupils as “friends” on any social media site.
- I am aware that when using my personal social media sites that I must make sure that I have appropriate privacy settings for my account as well as for specific content I share with others
- I am aware that, for my own protection, I should maintain a clear distinction between personal and professional uses
- I am aware that I must not use social media to connect with pupils in any way that allows me to access their personal information/data/images – or vice versa
- I will not communicate with any student using personal systems, including personal phones, or tablet devices and public web spaces (including, but not limited to, Facebook or X). The only exception may be when on official business (D of E; school trips).
- I am aware that when I use social media networking sites, what I say and the content I share is being put into the public domain. I am aware that I should not post comments or content that could cast me, the pupils, colleagues, the school or the Trust in a negative light. I am aware that the Trust may impose the Staff Disciplinary procedure in cases where a staff member has caused reputational damage or brought the school or Trust into disrepute.
- I will not use the Trust’s IT resources to access chat and social media networking sites using anything other than my work email address

Enabling all to flourish: Rooted in God’s love



- I understand that the Trust strongly advises I should have tight security on any social networking site of which I am a member and that I must protect my professional identity online
- I will not have any photographs or statements on public view that would put my professionalism into question
- I am aware that if, through using social media, I become aware of anything that gives me cause for concern about a student, I must report this to the Safeguarding Officer or a member of the SLT at earliest opportunity
- I am aware that if a student or parent makes contact with me via social media to discuss an individual matter, I should move this conversation off the social media platform and onto an established school channel (school email system or telephone)

11. Portable Electronic Devices and Laptops

All staff, governors and volunteers need to adhere to the below:

- 9.1 Ownership: The equipment remains the property of DSAMAT and must be returned when requested or at the end of employment. The device is provided for work purposes and should only be used for work. Use of the device must comply with the Data Protection Act, Computer Misuse Act and copyright laws.
- 9.2 Backup: Backing up and storing data on the device is your responsibility. You should conduct frequent back-ups of all data. In the event of a hardware or software fault, it may be necessary to reset the device to its original state resulting in loss of data.
- 9.3 Insurance: You will ensure that you take good care of the device and all reasonable precautions to ensure the device is not lost, stolen or damaged. The device is a part of the DSAMAT's insurance and inventory; therefore, you must comply with the following:
- Device within school: Your device must be locked away and secured at the end of a school day
 - Device within the home: Measures should be taken to keep the device safe within the home. It should be kept out of public view and away from hazards which could affect the performance or overall health of the device, such as wet or hot areas
 - Device within a vehicle: The device is insured during transit between school and home, and vice versa. The device must not be left unattended in a vehicle, even if it is in the boot
 - If a device is lost or stolen, you must inform Partnership Education. If the device is lost or stolen outside of school, then it is your responsibility to report the matter to the Police as well as to Partnership Education. Any Police paperwork should be shown to Partnership Education for inventory and insurance purposes
 - Devices must be made available to the relevant member of staff for Portable Appliance Testing

12. Law

- 10.1 Applicable laws (as amended) include, but are not limited to:
- GDPR Regulation 2016
 - Data Protection Act 1998/2018

Enabling all to flourish: Rooted in God's love



- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Obscene Publications Acts 1959 and 1964
- Protection of Children Act 1978
- Defamation Acts 1952 and 1996
- Public Order Act 1986
- Race Relations Act 1976
- Protection from Harassment Act 1997
- Telecommunications Act 1984
- Interception of Communications Act 1985
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

10.2 These Regulations apply subject to, and in addition to, the law. In all cases involving a breach of the law, criminal and/or civil sanctions may apply. Apart from the above and other relevant legislation, there may be other legal rights protected under common law, such as the law relating to confidential material or libel.

13. Monitoring and Review

- 13.1 The Board will approve all major changes to this policy.
- 13.2 The Trust has delegated the responsibility for implementing this policy to the Headteacher.
- 13.3 The policy will be promoted and published throughout the Trust by school leaders and those responsible for the induction and training of staff and volunteers.
- 13.4 The policy will be reviewed every three years or sooner if there are changes to the relevant legislation.



Appendix 1

ICT Acceptable Use Policy

I understand that I am responsible for my actions in and out of the work environment.

- I understand that this ICT Acceptable Use Policy applies not only to me whilst in work but also applies to my use of the Trust's IT infrastructure and equipment outside of work
- I understand that if I use internet based systems out of work that I must take care not to undertake any activity which contravenes any current legislation which could affect my employment within the Trust (including, but not limited to, offensive comments on social media sites, reposting of offensive or potentially inciting comments or images)
- I understand that my use of personal equipment in school is also covered by this policy
- I understand that any failure to comply with this ICT Acceptable Use Policy, could result in disciplinary action being taken.

I confirm that I have read and understood the ICT Acceptable Use Policy and will abide by the terms and conditions of use.

Employees of DSAMAT are asked to confirm the above via Handsam.

Local Governors, Directors and Members are asked to confirm the above through GovernorHub.