SAND
ACADEMIES TRUST
Supporting Achievement Nurturing Development

# IT Acceptable Use Policy

| Designation | Name | Date |
|---|---|---|
| Owner: | Mrs Lyn Dance (CEO) | |
| Author: | Mr Toby Ratcliffe (IT Manager) | |

| Monitoring and Evaluation | |
|---|---|
| Original implementation date: | July 2021 |
| Review frequency: | |
| Date of next Review: | |
| Review delegated to: | |

**Document Version control**

| Version | Changes made | Date |
|---|---|---|
| 1.0 | Initial set up of Trust-wide policy | July 2021 |
| 1.1 | CE Administrator account separation | Sept 2022 |
| | | |
| | | |
| | | |
| | | |

# Policy Statement

SAND Academies Trust (the Trust) has a combined IT Acceptable Use Policy for Equipment, Digital Communications, and Authentication (Passwords).

This policy aims to ensure appropriate access to, and use of, IT across the Trust, which will help to mitigate the following risks:

- Harm to individuals
- Damage to the Trust's reputation
- Potential legal action and/or fines against the Trust or individual(s)
- Inappropriate use of Trust resources
- Viruses and other malicious software
- Service disruption

# Scope

This policy applies to all employees, partners, contractors, agents of the Trust, and other third parties (users) who require any form of access to the Trust's information and information systems. This policy should be adhered to at all times when accessing information in any form and from any device. Questions regarding the content or application of this policy should be directed to the IT Helpdesk. Breach of this policy may be dealt with under the Trust's Disciplinary and Dismissals Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

# IT Equipment

## Things you Must Do

- Security and Access
  - ✓ Ensure that the Trust anti-virus software and security patches are updated on the laptop or PC on a regular basis. Laptops and PCs must be regularly connected to the internet.
  - ✓ Make backups of data when working offline by utilising OneDrive and connecting to the internet regularly.
  - ✓ Lock your laptop away out of sight when not in use, preferably in a lockable cupboard, filing cabinet, or safe (this also applies out of the office where possible).
  - ✓ Carry and store your laptop in a suitable padded carry bag or strong briefcase to reduce the chance of accidental damage.
  - ✓ Immediately report any suspected or observed security breach through the IT Helpdesk.
  - ✓ Keep personal use of IT equipment to a minimum.
  - ✓ Take account of the environment you are working in and ensure adequate security regardless of whether the laptop is used in the office, at home, in any other location, or while travelling.

- ✓ Contact the IT Helpdesk immediately if you receive a suspected virus or if you experience any unusual occurrences.

- Encryption
  - ✓ Ensure the laptop encryption is in use.
  - ✓ Use a strong encryption password / phrase /PIN in line with this policy.
  - ✓ Contact the IT Service if you are using a Trust owned device which is not enabled for encryption, in order for this to be resolved.
- Information and content
  - ✓ Take extra care when opening email attachments (the number-one source of computer viruses). Email attachments should not be opened unless the email comes from a trusted source and/or you were expecting it.

## Things you Must Not Do

- Security and Access
  - ✗ Disable, defeat, or circumvent any security measure that the Trust has put in place to protect the information assets, physical assets, or reputation of the Trust.
  - ✗ Keep encryption passwords and logon credentials with the laptop, or share them with any colleagues.
  - ✗ Use IT equipment for anything other than official Trust business or for generating, transmitting, or delivering any content that is contrary to Trust policies.
  - ✗ Leave IT equipment unattended at any time when outside the Trust premises including, but not limited to, in a car, briefcase, or handbag. If storing in a car is absolutely necessary , equipment should be locked out of sight in the boot or other compartment but it is generally much safer to take it with you.
  - ✗ Leave your laptop unattended and logged on. If not in use, it should be locked, logged out, or shut down.
  - ✗ Use IT equipment not procured through the IT service to store, use, or transfer any Trust information.
  - ✗ Allow your IT equipment to be used by work colleagues, family members, friends, or visitors – staff are personally accountable for anything accessed via their user ID.
  - ✗ Use any damaged or faulty IT equipment.
  - ✗ Transfer data using portable media, unless authorised.
- Administrators
  - ✗ Use administrator accounts for day to day tasks such as web browsing or accessing email.
- Copyright
  - ✗ Download or install any unauthorised accessories or software programs.
- Information and content
  - ✗ Send personal or special category information to a personal account or transfer it to removable media (including encrypted USB drives) for the purposes of remote working.
  - ✗ Send personal, special category, or other business related data via any Internet service(s) not supplied by the Trust without relevant permission.

# Digital Communications (Office 365)

## Things you Must Do

- Security and Access
  - ✓ Keep your personal use of the digital communication facilities to a minimum.
  - ✓ Assess the reliability of any information before using it (e.g. that it is from a reliable source, accurate, complete, and current).
  - ✓ Comply with the legal protections to data, images, and video provided by copyright and licenses.
  - ✓ Inform the IT Helpdesk immediately of any unusual occurrence (e.g. an antivirus software warning, getting pop-ups without having your browser open, unable to open files or task manager).
- Content
  - ✓ Take care to ensure that your communications (messages) are sent only to those who should receive them. Re-read messages before sending, check for correct addressing and clarity (particularly where they include personal or special category information), and ensure that the content will not embarrass or subject the Trust to legal proceedings or a fine.
  - ✓ Take care to ensure that any calls you make or receive cannot be overheard. You should be fully aware of your environment at all times, and avoid making calls that refer to personal or special category information in public places, over loud-speaker, or when using hands-free devices. You should also try to ensure that the recipient of your call takes these same considerations into account.
  - ✓ Put in place arrangements to ensure that incoming messages are dealt with during periods of planned absence.
  - ✓ Retain messages which constitute an official record in accordance with the Trust's Records retention and disposal schedule.
  - ✓ Exercise caution when opening emails and messages from an unknown external source or where, for any reason, they appear suspicious.

## Things you Must Not Do

- Security and Access
  - ✗ Send messages from another user's account or under an assumed name unless specifically authorised.
  - ✗ Respond to messages requesting personal information such as credit card details, user names or passwords, or containing links to internet sites where such information is requested.
  - ✗ Transmit any message or file attachments you know or suspect to be infected with a virus.
  - ✗ Access emails intended for others that are clearly marked 'personal' or 'addressee only' (for example when providing cover for periods of absence).
  - ✗ Allow third parties, contractors, or suppliers to remotely access/take over your PC or laptop via the internet.

- ✗ Subscribe to mailing lists for personal purposes using your Trust credentials, such as your email address.

- Personal, special category, and sensitive information
  - ✗ Upload personal or sensitive information into non-contracted systems, unless otherwise authorised, for example when required to provide information by law.
  - ✗ Send personal or sensitive information by non-secure means, unless otherwise authorised, for example where the service user is aware of the risks and has requested communication by other means.
  - ✗ Forward personal, special category, or sensitive information to an external location (including your personal home email address) or to another person who may not be authorised to see the information.
- Content
  - ✗ Create, download, upload, display, or knowingly access sites that contain, or might be deemed to be:
    - Pornographic
    - Illegal
    - Obscene or offensive (discriminatory, or of an extreme political nature)
    - Subversive or violent.
  - ✗ Send messages, or create or send content, that violates the privacy of, or unfairly criticises others, or that may damage the Trust's reputation, unreasonably waste staff resources, or disrupt the work of other email users.
  - ✗ Inadvertently send messages containing statements which are likely to create liability (whether criminal or civil, and whether for you or the Trust).
  - ✗ Send commercial or advertising material, chain letters, or junk mail (otherwise known as spam) of any kind.
  - ✗ Click on links or attachments within emails or messages from unknown or suspicious external sources (for example if the attachment ends in .exe)
- Subscriptions and contract terms
  - ✗ Subscribe to, enter or use online gaming or betting sites.
  - ✗ Subscribe to or enter 'money making' sites or enter or use 'money making' programs.
  - ✗ Agree to terms, enter into contractual commitments or make representations unless appropriate authority has been obtained.
- Private use
  - ✗ Use the Trust's internet or digital communication facilities to order/purchase goods and services for personal use.
  - ✗ Personally subscribe to or use: real time chat facilities such as chat rooms, instant messaging, or social networking sites such as Facebook or Twitter with your Trust credentials.
  - ✗ Undertake any private buying, selling or monetary transactions e.g. online trading using sites such as eBay, or personal bank account transactions using Trust facilities.
  - ✗ Use Trust facilities to run a private business.

# Authentication (Passwords)

## Things You Must Do

- ✓ Ensure that your password is not divulged or shared with anyone else.
- ✓ Change your passwords in line with this policy.
- ✓ Change your password immediately if you believe your password(s) may have been compromised.
- ✓ Create different passwords for your various Trust accounts.
- ✓ Be aware that different applications may enforce varying password complexity.
- ✓ Optionally use biometric authentication as an ease of access method e.g. Face ID or Touch ID.

## Things You Must Not Do

When using the Trust's information or information systems you must NOT:

- ✗ Write down and store passwords within the office i.e. in office diaries or paper files.
- ✗ Reveal passwords over the phone.
- ✗ Reveal passwords on questionnaires or security forms.
- ✗ Hint at the format of a password (for example "my family name").
- ✗ Use existing personal account passwords for any Trust accounts (e.g., personal internet (ISP) accounts, banks, etc.) or vice versa.
- ✗ Insert passwords into email messages. (Systems-generated temporary passwords are regarded as an exception and can be emailed as these are classified as temporary passwords and must be changed as soon as possible).