SOUTH LINCOLNSHIRE ACADEMIES TRUST (SLAT)

IT & Network Policy

Aspire - Challenge – Achieve

Author	Link	Date Approved
Chief Operating Officer	Chief Executive Officer	Jan - 26
Policy Type	**Date of Next Review**	**Approved By**
Trust Wide	Jan - 27	Trust Board of Directors

South Lincolnshire
Academies Trust

IT POLICY

This policy has been written to protect the computer network and intellectual property from unauthorised or unlawful use. Staff and students are expected to adhere to this policy throughout their employment.

ROLES AND RESPONSIBILITIES

Chief Executive Officer

It is the responsibility of the Chief Executive Officer to ensure that;

- This policy is implemented across the Trust.
- This policy is appropriately communicated to all staff across the Trust.
- Specialist help and assistance is sought if required.
- Significant occurrences are reported to Trust Board of Directors

Chief Operating Officer

It is the responsibility of the Chief Operating Officer to ensure that;

- The arrangements below are effective.
- Ensure access to the network is authorised.
- The arrangements below are proportionate and appropriate.
- Reviews are undertaken after a significant occurrence (e.g. CyberAttack).
- Any remedial action or findings after a significant occurrence is implemented.

Director of IT Infrastructure

It is the responsibility of the Director of IT Infrastructure to ensure that;

- Any concerns regarding the integrity of the network system is raised with the Chief Executive Officer or Chief Operating Officer.
- This policy is implemented across the IT Support team.
- To act in the best interests of the IT Infrastructure & Network when deemed appropriate.
- To monitor all network activity for accidental or deliberate intrusion of secure systems.
- To report any suspicious activity, either internal or external to the Chief Executive Officer or Chief Operating Officer.

COMPUTER ETHICS, COPYRIGHTS AND INTELLECTUAL PROPERTY

Staff and students are prohibited from making copies of any programs stored on any Trust desktop or server.

The Director of IT Infrastructure is the only authorised member of staff who can make backup copies of software for which the Trust has licences, only for the purpose of retaining a copy of the software to protect the original data and for the purpose of which the software was purchased.

Staff and student should be aware of resources that are protected by copyright; to use text, images, sounds, video, scripts and other objects on and off web pages without the appropriate credit and permission from the owners.

Computer software is protected by UK and International Copyright law and is subject to criminal prosecution which includes heavy fines and imprisonment.

COMPUTING RIGHTS AND RESPONSIBILITIES

Computers and networks *are the property of South Lincolnshire Academies Trust* and can provide access to teaching materials on and off site, which is therefore regarded as a privilege and not an expectation.

Director of IT Infrastructure has the right to protect the integrity of the Trust network and resources from harmful attacks.

Under no circumstances must food or drink be brought into any computing/ICT resource area within the Trust.

Electronic mail (email) is an extremely powerful tool and must not be abused by spamming or sending commercial or unacceptable materials to any user on the Trust network or, any other inter-networked system whilst operating from the Trust's network.

If access to a network account or email account is required in a situation where the member of staff or student is unavailable, for example; illness or to form part of a personnel investigation the Chief Executive Officer and Chief Operating Officer can authorise access to various parts of the network to be released and/or accessed to other senior members of staff.

Malware and Virus protection software is there for the user's protection; therefore, settings must not be tampered with.

The Chief Operating Officer and Director of IT Infrastructure reserve the right to exclude user's access to rooms or resources in the event of a system breach.

Personal storage space will be scanned for viruses and illegal content, any software deemed to be illegal may result in disciplinary action.

Under no circumstances should any IT equipment be moved, relocated or unplugged without the consent of the IT Support team.

Staff and students are reminded that the use of the network is for work related tasks, accessing personal emails, bank accounts, social media etc. is strictly prohibited. Staff email addresses should only be used in association with work related accounts, using these email addresses to register for personal, non-work related reasons is also prohibited.

The 'releasing' of accounts, shall be logged by the IT Director or IT Manager.

LEGAL ISSUES

Users have the right to access information held about themselves on computer files as stated in the Data Protection Act 2018 accompanied by UK GDPR

Users may be held accountable for their conduct while operating any Trust IT resource.

Complaints alleging misuse of computing and networking resources will be directed to the Director of IT Infrastructure or any authorised member of staff who would be responsible for taking appropriate disciplinary action.

Any user found trying to hack/crash or breach any Trust computer system or soliciting with hackers will be immediately banned from using any of the Trust's computing resources in the future and risk prosecution under the Computer Misuse Act 1990 (UK).

CCTV (CLOSED CIRCUIT TELEVISION)

Users must be aware they are monitored by CCTV systems for the purposes of Security and Safety. Areas that are monitored by CCTV will be recorded. Footage will be held for a period of time dependant on the VDR box capability. A log will be kept of any material that is reviewed. It will include the reason for review, when it was reviewed and by whom.

The viewing of live or recorded footage is restricted to a small number of staff. No member of staff or student is authorised to view, attempt to view or making attempts to access CCTV system without clear authorisation from the Chief Executive Officer, Chief Operating Officer or Director of IT Infrastructure. See CCTV policy for more information.

MISUSE OF COMPUTING & NETWORK RESOURCES

Examples of misuse include, but are not limited to, the activities in the following list:

- Sharing your username/password(s) or access to any of your Trust computing accounts unless authorised to do so;
- Using a computer account or obtaining a password for a computer account that you are not authorised to use;
- Deliberately viewing or creating obscene or indecent material (including but not limited to that which portrays sex, nudity, violence or suffering in a gratuitous manner);
- Knowingly installing third party software onto any computer system or network within the Trust without authorisation from the Director of IT Infrastructure;
- Using Trust computing resources for commercial activities in violation of the Trust policy;
- Using copyrighted text, images, sounds, video without proper credit to and permission from the owner;
- Using email to harass others and/or pass chain letters to others;
- Sending Selective Promotion Advertising Mail (SPAM) to large groups of users, either on or off site;
- Attempting to monitor or tamper with another users account;
- Reading, copying, changing or deleting another user’s files or software without the owner’s explicit consent;
- Using any Trust computing resource to gain unauthorised access to any computer system;
- Revealing confidential information obtained from administrative data systems to unauthorised people or groups, e.g. a SIMS.net profile record;
- Attempting to circumvent data protection schemes or uncover security loopholes;
- Violating terms of applicable software licensing agreements or copyright laws;
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojans and worms.
- Sending or distributing emails for reasons not related to work.
- Deliberate physical damage to computer or network device will be resolved in accordance with the South Lincolnshire Academies Trust Behaviour Policy.
- No software or services should be purchased or subscribed to without prior authorisation. Authorisation and approval will be from the Director of IT Infrastructure once relevant compatibility, security checks etc have been carried out, and to ensure we also maintain an update to list of where school data may reside. Once authorised the SLAT Finance Handbook should be followed correctly, before software is obtained.

MOBILE DEVICES

Mobile devices e.g. mobile phones and tablets may be used to access Trust information systems. These devices and/or systems must be password protected and not automatically sign in.

Any incident that may lead to unauthorised access to Trust information must be reported to the Police.

STUDENT’S PERSONAL DATA

All electronic data including personal storage space and email shall be deleted 30 days after completion of course or program of study.

Applications for the extension of the 30-day period will be considered on receipt of a written explanation to be lodged with the Network Managers, no later than 7 days prior to completion of your course or program of study within the Trust.
This policy should be read in conjunction with the Trust UK GDPR Policy.

PERSONAL DEVICES & ACCESS

Personal wireless device access is restricted to Internet only. Users will not have access to any documents which reside on the Trust network directly but will be able to access documents via the Trust remote access system. Internet traffic will be filtered in the same way that Trust local area network traffic is filtered.

Access to the South Lincolnshire Academies Trust guest wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all Trust rules. The use of the network also allows IT support staff to conduct investigations regarding inappropriate Internet use at any time.

ACCESSING THE WIRELESS NETWORK

Students should search for the guest wireless networks and will be prompted to log on. They will then be prompted to enter their username and password, which is the same username/ password they enter to access the schools network.

The first time your device is connected to the network, you must install the Security Certificate as mentioned on the login page. Download the file, open and accept all the default prompts to install. If you have any issues connecting, please contact the IT Technicians.

GUIDELINES FOR STUDENTS

The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons e.g. contacting parents, should only take place outside of taught time and tutor time in the sixth form centre for Post 16 students.

Do not share your username or password with anyone and do not connect anyone else’s device to the network using your username or password.

The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class or private study areas in any way.

Users shall make no attempts to circumvent the Trust network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

Users shall not take or distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

Users are not permitted whilst connected to the Wi-fi to carry out

- Gaming
- Online gaming
- Peer to peer file sharing (including, but not limited to the use of torrent)
- Video and audio streaming of a non-educational nature

There are no secure facilities provided at school to store personal ICT devices. Students should therefore keep their personal device with them at all times.

ACADEMY LIABILITY STATEMENT

Students, members of staff and visitors bring their devices to use entirely at their own risk. The school will NOT be liable for any (hardware or software) loss, damage, malfunction or inconvenience to the electronic device arising directly or indirectly as a result of its connection to the Trust network system. It is their own responsibility to ensure that any software installed on the device is correctly licensed. They are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

INSURANCE

South Lincolnshire Academies Trust is in no way responsible for:

- Personal devices that are broken while on site.

- Personal devices that are lost or stolen.
- Data lost on personal devices
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

Users should ensure that their electronic device is suitably insured.

USE OF CLOUD STORAGE

South Lincolnshire Academies Trust advise all users to use the relevant 'Drive' when working on the network. Use of cloud storage on the network is permitted, but it is also exempt from Trust wide backups. Local storage is backed up daily in accordance with Trust IT and Network Operating procedures, however owing to accessibility and external constraints cloud backups are not taken. Staff and students work on cloud-based storage at their own risk and are discouraged not to.

Appendix 1.0

BRING YOUR OWN DEVICE STUDENT AGREEMENT

I ________________________________ confirm I have read and fully understood the South Lincolnshire Academies Trust IT & Network Policy. I will follow all of the guidance stated and understand that the Wireless Fidelity system is a privilege and not an entitlement. I understand that any breach or attempt to breach of this policy will result in me *(above named)* losing all access to the Trust wireless systems.

- I am aware that my own device will be monitored by South Lincolnshire Academies Trust IT staff.
- I am aware that some breaches of this policy for example, downloading torrented media, may require involvement from external agencies
- I am aware that I am responsible for my own device, and its use by other students.
- I am aware that I am responsible for any damage, theft or loss of my device.
- I am aware that I must use the WiFi system in accordance with this policy.
- I am aware that I must not use or attempt to use a VPN.
- I understand that my access to the Trusts WiFi is for educational purposes
- I can confirm that I have Anti-Virus installed and is fully up to date.

Signed:

Date: