

SOUTH LINCOLNSHIRE ACADEMIES TRUST (SLAT)

IT Policy - Staff

Aspire - Challenge – Achieve

Author	SLT Line Link	Date Approved
H Lewis		February 2021
Policy Type	Date of Next Review	Approved By
Trust Wide	February 2023	Trustees



South Lincolnshire

Academies Trust

IT POLICY

COMPUTER ETHICS, COPYRIGHTS AND INTELLECTUAL PROPERTY

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

Only IT system staff are authorised to 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 purpose for which the software was purchased.

Users of the Trust's resources must understand that it is a breach of 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.

South Lincolnshire Academies Trust IT system administrators have the right to protect the Trust's Intranet and Internet facilities to ensure that they abide by the terms and conditions of our provider.

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 must not be abused.

IT system administrators reserve the right to protect the integrity of the Trust's 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's network or, any other inter-networked system whilst operating from the Trust's network.

If an employee is absent from work for any reason and it is deemed computer access is required, the Executive Headteacher reserves the right to authorise such access.

Anti-Virus software is there for the user's protection; therefore settings must not be tampered with.

IT system administrators 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 taken against offenders.

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

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 ICT resource.

Complaints alleging misuse of computing and networking resources will be directed to the Network Managers 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.

EXAMPLES OF MISUSE OF COMPUTING & NETWORK RESOURCES

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

- Giving anyone 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 Network Manager;

- Using Trust computing resources for commercial activities in violation of the Trust's 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;
- 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.

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, the Operations Manager and the Network Manager.

STUDENT'S PERSONAL DATA

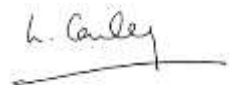
Electronic backup facilities can be accessed by contacting the IT Support Department.

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's Data Protection Policy.

Approved



Date _____

Mrs L Conley - Executive Headteacher

