Information Systems Policy

Aim of the Trust

One community. Many ideas. Everyone's future.

We aim to provide an exceptional education for every child in the Trust through an ethos of collaboration and high aspirations and through the principles of quality learning using curiosity, exploration and discovery.

The information systems policy covers the use of the Trust's computer systems (hardware, software, data, telephone network, computer network, email and internet) by all staff, and the use of online tools provided by the Trust. This policy consists of three sections:

1. Acceptable use of ICT equipment

2. Use of telephones, email and internet by staff

3. Safe use of online resources

This policy is linked to:

- Staff Discipline Policy
- E-safety Policy
- Staff Code of Conduct Policy
- Data Protection Policy
- GDPR Privacy Statement for Employees

1. **Acceptable use of Computer Systems: Principles**

The Trust is committed to safeguarding its computing system to ensure it can be used in the most effective manner to support the teaching and learning processes and enable The Trust's business tasks to be undertaken. Ensuring the safety and integrity of the Trust's ICT system is the responsibility of all staff.

The Trust encourages staff to fully use the computing infrastructure and to make use of Mobile Computer Devices equipment offsite to support them in their work. The Trust encourages this use in a responsible and professional manner. Mobile devices include for example laptops, tablets, notebooks, smartphones and other portable/mobile devices.

As a user of the Trust's Computer systems you have a right to use it responsibly. These user responsibilities are outlined below. Misusing the Trust's computing systems may breach this and other Trust policies.

Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Staff are advised of this policy during their induction and of the Trust's requirement for them to adhere to the conditions therein.

For the purposes of this policy the term "computing services" refers to any computing resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet). Staff who connect their own device to the Trust's network and the services available are particularly reminded that such use requires compliance to this policy.

Purposes

• To protect the Trust's networks and equipment

• To protect the Trust's data

• To protect the Trust and its employees from activities that might expose them to legal action from other parties

Guidelines

Password security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the Trust.

Issuance and continued use of your User Account is conditional on your compliance with this policy.

User ID's and passwords must not be shared or revealed to any other party. Staff must assume personal responsibility for usernames and passwords for all accounts and sites connected with their employment at the Trust. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy.

Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords are set by policy to expire every 3 months so users are forced to change their passwords. Passwords should be changed immediately if the user believes or suspects that their account has been compromised.

General Conditions

In general, use of Trust "computing services" should be for your/the user's study, research, teaching or the administrative purposes of the Trust. Some use of the facilities and services for personal use is accepted, so long as such activity does not contravene the conditions of this policy.

• Your use of the Trust's computing services must at all times comply with the law.

• Your use of the Trust's computing services must not interfere with any others' use of these facilities and services.

• You are not entitled to use a computer/device that you have not been authorised to use.

• You must not access any program or data which has not been specifically authorised for your use.

• You must not use or copy any data or program belonging to other users without their express and specific permission.

• You must not alter computer material belonging to another user without the user's permission.

• You must not use Trust computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.

• You must not use Trust computing services for the creation, modification, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Headteacher).

• You must not use the Trust's computing services to conduct any form of commercial activity without express permission.

• You must not use the Trust's computing services to disseminate mass (unsolicited) mailings.

• You must not install, use or distribute software for which you do not have a license, and which is not first authorised by the ICT technicians for installation

• You must not use any P2P/torrent client as these enable illegal sharing of copyrighted material

• You must not use any IRC or messenger software including, but not limited to WhatsApp, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorised to do so for work related purposes

You must not use any Messenger Software, including but not limited to WhatsApp, Hangouts, Internet Relay Chat (IRC), unless authorised to do so from the Principal for work related purposes.

• You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the Trust facilities, unless specifically related to Trust activities

• You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Executive Principal/Governing Board

• You must not play computer games of any nature whether preinstalled with the operating system or available online unless it has been agreed by your line manager as having educational value for children or it is outside of your working hours

Data Security

The Trust holds a variety of sensitive data including personal information about students/pupils and staff. If you have been given access to this information, you are reminded of your responsibilities under the Data Protection Act 2018 and General Data Protection Regulations 2018 (GDPR).

You should only take a hard copy of data outside the Trust's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, any removable encrypted storage device, and cloud storage or into secure emails, also personal cloud storage solutions (example: MS OneDrive, Google drive, iCloud) for the transfer of Trust information is expressly forbidden. Use of cloud storage must be authorised by the Data Protection Officer. If you do need to take data outside the Trust, this should only be with the authorisation of the Trust's Data Protection Officer. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular using VPN and remote desktop or terminal services) which allow you to work on data in-situ rather than taking it outside the Trust, and these should always be used in preference to taking data off-site.

The ICT Technicians offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

Anti-Virus and Firewall Security

All Trust devices are installed with current versions of virus protection and firewall software by the ICT Technicians. Users cannot alter the configuration of this software and no attempt should be made to do so by any means. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, they should inform the ICT Technicians immediately. If the ICT Technicians detects a machine behaving abnormally due to a possible viral infection it will disconnected from the network until deemed safe.

Physical Security

The users of computing equipment should always adhere to the following guidelines:

• Treat equipment safely, in the same manner as a reasonable person would

• Keep liquids away from ICT equipment

• Do not place heavy objects on ICT equipment

• Do not drop ICT equipment or objects onto it

• Any portable computer must be securely locked away when not in use

• Portable computer security is your responsibility at all times

• Do not leave the portable computer unattended in a public place or within the Trust

• Do not leave the portable computer inside your car

• Extra reasonable care must be taken to prevent the loss of any removable storage device which contain confidential Trust data

• Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment

Remote Access

Remote access to the Trust network is possible where this has been granted by the ICT Technicians.

Remote connections are considered direct connections to the Trust network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available to the Network Manager and ICT Technicians and kept for no longer than necessary and in line with current data retention schedule.

Such records and information are sometimes required - under law - by external agencies and authorities. The Trust will comply with such requests when formally submitted.

Breaches of this Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

In the event a Portable Computer/ Mobile Device is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the Trust.

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

• Taking food and/or drink into rooms with computing facilities where they are forbidden

• Sending nuisance (non-offensive) email

• Behaving in a disruptive manner

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of non-compliance would include:

• Repeated minor breaches within the above detailed 12-month period

• Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area

• Assisting or encouraging unauthorised access

• Sending abusive, harassing, offensive or intimidating email

• Maligning, defaming, slandering or libelling another person

• Misuse of software or software license infringement

• Copyright infringement

• Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Examples of this level of breach would include but are not limited to:

• Repeated moderate breaches

• Theft, vandalism or willful damage of/to Computing facilities, services and resources

• Forging email i.e. masquerading as another person

• Loading, viewing, storing or distributing pornographic or other offensive material

• Unauthorised copying, storage or distribution of software

• Any action, whilst using Trust computing services and facilities deemed likely to bring the Trust into disrepute

• Attempting unauthorised access to a remote system

• Attempting to jeopardise, damage circumvent or destroy Computing systems security

• Attempting to modify, damage or destroy another authorised users data

• Hacking into the Trust's network infrastructure to disrupt network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process

An investigation will be carried out, in confidence, by Leadership under the direction of the Headteacher/Executive Principal. That investigative report will be passed to the staff member's Line Manager, to be considered within the Trust's disciplinary procedures. Each set of disciplinary procedures provide for an appeal stage.

2. Use of telephones, email and internet by staff

Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the internet on a device. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This Policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the Internet.

The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedure.

This Policy has been designed to safeguard the legal rights of members of staff under the terms of the Data Protection Act, GDPR and the Human Rights Act.

Purposes

To provide guidance on inappropriate use of Trust telephones, email and internet facilities.

To clarify when the Trust may monitor staff usage of these facilities.

Guidelines

Use of telephones

There will be occasions when employees need to make short, personal telephone calls on Trust telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of Trust telephones for private purposes, which are unreasonably excessive or for Trust purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the Trust has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the Trust reserves the right to record calls.

Use of email

As with telephones it is recognised that employees can use e-mail for personal means in the same manner as that set out for telephones above. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.

Employees should be careful that before they open any attachment to an e-mail they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the Trust. Any other use of e-mail for either personal or Trust purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure.

Where the Trust has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The Trust also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the Internet

The primary reason for the provision of internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their Trust role. However, it is legitimate for employees to make use of the Internet in its various forms in the same way as email above as long as

it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. The Trust reserves the right to audit the use of the Internet from particular Personal Computers/devices or accounts where it suspects misuse of the facility

Use of personal devices

Where staff use their own personal equipment such as mobile telephones, laptops, notebooks, tablets etc, if they are on Trust premises, or being used to access Trust data from anywhere, this must be with the permission of the Trust and the devices must be secure with confidential passwords.

Monitoring the use of telephone, e-mail and the Internet

It is not the Trust's policy, as a matter of routine, to monitor an employee's use of e-mail service or of the Internet via the Trust's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Executive Principal or Governing Board may grant permission for the auditing of an employee's telephone calls e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Headteacher/Executive Principal.

These individuals are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Executive Principal/Governing Body or their delegated representative to enable Human Resources to advise the appropriate line manager/head of faculty the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

3. Safe use of Management Information Systems

Principles

This applies wherever access to the Trust Management Information Systems (MIS) are provided. This applies to all online resources provided by the Trust, for example Capita SIMS. This policy applies whenever information is accessed through the Trust MIS, whether the computer equipment used is owned by the Trust or not. The policy applies to all those who make use of the Trust's MIS resources.

Purposes

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of the Trust's data, the Authorised MIS User and the individuals to which the MIS data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials
- The wrongful disclosure of private, sensitive, and confidential information
- Exposure of the Trust to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

This Policy aims to ensure all relevant aspects of the Data Protection Act (2018) and GDPR (2018) are adhered to.

This Policy aims to promote best use of the MIS system to further the communication and freedom of information between the Trust and Parents/Carers.

Guidelines

The Trust's MIS system is provided for use only by persons who are legally responsible for student(s)/pupils currently attending the Trust. Access is granted only on condition that the individual formally agrees to the terms of this Policy.

The authorising member of Trust staff must confirm that there is a legitimate entitlement to access information for students/pupils the names of whom must be stated on the Online Usage Policy Declaration.

A copy of the form will be held by the Trust for audit purposes.

Personal Use

Information made available through the MIS system is confidential and protected by law under the

Data Protection Act 2018, and GDPR. To that aim:

Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the student/pupil to which the information relates or to other adults with parental/carer responsibility.

Best practice is not to access the system in any environment where the security of the information contained may be placed at risk.

Questions, Complaints and Appeals

MIS users should address any complaints and enquiries about the MIS system to the Trust in writing to the Network Manager and Executive Principal.

The Trust reserves the right to revoke or deny access to MIS systems of any individual under the following circumstances:

• The validity of parental/carer responsibility is questioned

• Court ruling preventing access to child or family members is issued

• Users found to be in breach of this policy

If any child protection concerns are raised or disputes occur the Trust will revoke access for all parties concerned pending investigation.

Please note: Where MIS access is not available the Trust will still make information available according to the Data Protection Act (1998) and GDPR. For more information relating to data retention please see Appendix 1 – Data Retention Schedule

Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

Upon leaving the Trust, members of staff must return all equipment and information, including equipment and data on or before the agreed leaving date (eg last day of employment) to their Line Manager or other Academy representative. This includes, but is not limited to:

All information, including data, used or stored as part of the role, both physical and electronic.

All information, including files, documents and emails, including any data stored within individual accounts

Access control and ID cards

After leaving members of staff may not attempt to access or use any Academy information, including any data.

The Langley Academy Trust

Computing Services Declaration

Please only sign if you have fully read this Information Systems policy. By signing the declaration form you are agreeing that you have fully understood the terms and conditions and all the instructions/policies of the Trust Computing Services.

Please contact the Trust Network Manager if you are not sure of any policies and terms and conditions of use.

Declaration

I hereby confirm that I have read and fully understood the terms and conditions document attached and will strictly follow the policies of the Langley Academy Trust Computing Services

Signature……..

Staff/Governor/Trustee/Volunteers Name……..

Parent/Carer Name……

Child(ren) Name(s)……Year /Class)…….....

Child(ren) Name(s)……Year /Class)…….....

Child(ren) Name(s)……Year /Class)…….....

Date…….

Review Date: June 2019

Ratified Date: June 2019

Author: Rhodri Bryant

Date of next review: June 2022