Information Systems Policy

Aim of the Academy
To provide unique and enriching opportunities for all.

The information systems policy covers the use of ICT systems to support learning, the use of telephones, email and the internet by staff, and the use of online tools provided by The Langley Academy. 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

1. Acceptable use of ICT

equipment Principles

The Langley Academy is committed to safeguarding its ICT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the academy's ICT infrastructure is the responsibility of all staff.
The academy encourages staff to fully use the ICT infrastructure and to make use of portable ICT equipment offsite to support them in their work. The academy encourages this use in a responsible and professional manner. Portable computers include for example laptops, tablets and other portable ICT devices.
As a user of ICT services of the academy you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse academy computing facilities in a way that constitutes a breach or disregard of this policy, consequences associate with that breach and you may be in breach of other academy regulations.
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 academy's requirement for them to adhere to the conditions therein.
For the purposes of this policy the term "computing services" refers to any ICT 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 ICT to the Academy's network and the services available are particularly reminded that such

use requires compliance to this policy.

Purposes

- To protect the academy's networks and equipment
- To protect the academy's data
- To protect the academy 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 Academy. Issuance and continued use of your User Account is conditional on your compliance with this policy. User ID's and passwords are not to be shared or revealed to any other party. 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 should be routinely changed (every 3 months is recommended) and should be changed immediately if the user believes or suspects that their account has been compromised.

General Conditions

In general, use of academy "computing services" should be for your study, research, teaching or the administrative purposes of the academy. Modest 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 academy's computing services must at all times comply with the law.
- Your use of the academy's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer 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 users' permission.
- You must not use academy computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use academy computing services for the creation, 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 Principal).
- You must not use the academy's computing services to conduct any form of commercial activity without express permission.
- You must not use the academy's computing services to disseminate mass (unsolicited) mailings.

- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by the ICT Department for installation
- You must not use any peer-to-peer file sharing software
- You must not use any IRC or messenger software including, but not limited to AOL, MSN, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorized to do so for work related purposes
- You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the academy's facilities, unless specifically related to academy 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 Principal/Governing Board
- You must not play computer games of any nature whether preinstalled with the operating system or available online

Data Security

The academy holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law.
You should only take a copy of data outside the academy's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, memory sticks, cds/dvds or into emails. If you do need to take data outside the academy, this should only be with the authorisation of the academy'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 Academy, and these should always be used in preference to taking data off-site.
The ICT Department 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 personal computers are installed with current versions of virus protection and firewall software by the ICT Department. Users are not to alter the configuration of this software unless express permission has been obtained from the ICT Department. 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 Department immediately. If the ICT Department 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 ICT 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 academy
- Do not leave the portable computer on view inside your car. It should be locked away in your car's boot out of sight.
- Extra reasonable care must be taken to prevent the loss of USB sticks which contain confidential academy data
- Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment

Remote Access

Remote access to the academy network is possible where this has been granted by the ICT Department.
Remote connections are considered direct connections to the academy 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 only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.
Such records and information are sometimes required - under law - by external agencies and authorities. The academy 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 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 academy.

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 ICT 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 licence 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:

- Repeated moderate breaches.
- Theft, vandalism or willful damage of/to ICT 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 academy computing services and facilities deemed likely to bring the academy into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy ICT systems security.
- Attempting to modify, damage or destroy another authorised users data
- Disruption of 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 academy Leadership under the direction of the Principal. That investigative report will be passed to the staff member's Line Manager, to be considered within the academy'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 personal computer. 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 as well as the academy Acceptable Use and academy Security Policies.
This Policy has been designed to safeguard the legal rights of members of staff under the terms of both the Data Protection Act and the Human Rights Act.

Purposes

To provide guidance on inappropriate use of academy telephones, email and internet facilities.
To clarify when the academy 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 academy 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 academy telephones for private purposes, which are unreasonably excessive or for academy purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.
Where the academy 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 academy 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 a personal 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 academy. Any other use of e-mail for either personal or academy 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 academy 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 academy 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 academy 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 academy reserves the right to audit the use of the Internet from particular Personal Computers or accounts where it suspects misuse of the facility

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

It is not the academy's policy, as a matter of routine, to monitor an employee's use of the academy's telephone or e-mail service or of the Internet via the academy'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 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 Principal. These staff 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 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 online resources

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

Purposes
Security

- This Policy is intended to minimise security risks. These risks might affect the integrity of The Langley Academy'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 Langley Academy 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 (1998) and Fair Processing Policy are adhered to.
- This Policy aims to promote best use of the MIS system to further the communication and freedom of information between The Langley Academy and Parents/Carers.

Guidelines

The Langley Academy's online systems are provided for use only by persons who are legally responsible for student(s) currently attending the academy.

Access is granted only on condition that the individual formally agrees to the terms of this Policy.

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

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

Personal Use

Information made available through the MISsystem is confidential and protected by law under the Data Protection Act 1998. 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 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.

Password Policy

Staff must assume personal responsibility for usernames and passwords. Never use anyone else's username or password.

You must always keep your individual user name and password confidential. These usernames and passwords should ***never*** be disclosed to anyone. Passwords and user names should never be shared.

In some instances users may be given the right to change passwords from the one originally issued..

Questions, Complaints and Appeals

MIS users should address any complaints and enquiries about the MIS system to The Langley Academy in writing to The Head of ICT.

The Langley Academy 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 academy will revoke access for all parties concerned pending investigation.

Please note: Where MISaccess is not available The Langley Academy will still make information available according to Data Protection Act (1998) law.

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.

The Langley Academy

Computing Services Declaration

Please only sign if you have fully read the Information Systems policy. By signing the acceptance form you are agreeing that you have fully understood the terms and conditions and all the instructions/policies of The Langley Academy Computing Services.
Please contact The Head of ICT at The Langley Academy 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 usage of The Langley Academy computing services.

Signature_____*

Parent/Carer Name_____*

Child(ren) Name(s)_____ * Year_____*HTG_____*

_____ Year_____HTG_____

_____ Year_____HTG_____

Address_____*

Email address_____*

Mobile number_____*

*MUST BE COMPLETED

Review Date: May 2013
Ratified Date: 12 June 2013
Date of next review: June 2019