THREE LANE ENDS ACADEMY

Acceptable Use Policy 2019

Adopted by Governing Body on: January 2019

Reviewed date: January 2020

Three Lane Ends Academy
Information and Communication Technology Acceptable Use Policy

Contents

Introduction

Three Lane Ends acceptable use policy is divided into the following four sections.

1) General policy and code of practice
2) Internet policy and code of practice
3) E-mail policy and code of practice
4) Social media use – see also the Academy's 'E-Safety Policy'

This document covers academy ICT facilities and all electronic information and data in use by or relating to the academy with particular respect to email and internet security. The same policies and guidance applies when accessing Three Lane Ends Academy systems remotely.

Scope

The policy covers:

- All employees of TLE Academy
- All voluntary workers that are given access to the use of academy computer equipment
- ITT/School direct and work experience pupils
- Third party users such as Supply staff / Deaf & Hearing Impaired Staff
- Pupils, parents and Governors (where applicable)
- All hardware and software purchased by the academy for academy use by the above user groups

TLE Academy actively encourages the use of ICT facilities within the academy and is continually working to improve and extend ICT services for the benefit of teaching and learning alike. TLE Academy wants to promote best practice and responsible use of ICT facilities throughout the Academy.

Updates to this policy

Updates to the policy or supplements may be added and made available to staff either in paper or electronic format. Amendments must be adhered to and are agreed to by the act of signing the original document.

Privacy

In particular please note the provisions set out in this ICT policy about privacy and how the academy may monitor data, information and material in relation to or used, sent or received by you.

Section One - General Policy and code of practice

Introduction

The academy has well-developed and advanced ICT systems, which it intends that you will use and benefit from. The policy set out below sets out the rules that you must comply with to ensure that the system works effectively for everyone.

PRIVACY

The academy will try to respect your privacy but in order to protect pupils' safety and well-being and to protect the academy from any third party claims or legal action against it, the academy may view any data, information or material on the academy's ICT system (whether contained in an e-mail, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. You consent to the academy viewing, using and disclosing data, information or material in relation to, used, sent or received by you.

The academy disclaimer which automatically appears at the end of each of your e-mails notifies the recipient that any e-mail correspondence between you may be monitored. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an e-mail that the academy may monitor the content of his e-mail.

You should never disclose information about the academy ICT facilities or personal data to anyone unless on Academy business.
The storage and processing of personal information about pupils is governed by the Data Protection Act (2018).

Code of practice

Academy's philosophy	In using ICT, you will follow the academy's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
Times of access	The network is available during term time. Out of term time the network will be subject to maintenance downtime and so may not be available for brief periods.

User ID and password and logging on	You will be given your own user ID and password. You must keep these secret and not tell or show anyone what they are. Your password should be at least six characters long and a mixture of capitals, lower case letters, numbers and symbols. If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the ICT support staff. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. The academy's system records, and senior ICT staff monitor, the use of the system. Use of the academy's facilities by a third party using your user name or password will be attributable to you, and you will be held accountable for the misuse. **You must lock your computer when you leave it unattended.** TLE Academy reserves the right to request you change your password.
Printing	The Academy may wish to check that expensive resources are being used efficiently and the member of staff may suggest other strategies to you in order to save on resources.
Logging off	You must either lock or log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. This signals to the system that you are no longer using the service, it ensures security and frees up resources for others to use.
Access to information not normally available	You must not use the system or the internet in order to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. If you feel that you have accidentally accessed an area of the network that you think you should not be able to access you must alert the ICT Network Manager immediately. You must not attempt to install software to explore or harm the system. Use of hacking tools e.g. 'loggers', 'sniffers' or 'evidence elimination software' is expressly forbidden.
Connections to the system	You must not connect any hardware which may be detrimental to the academy network.

Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the written permission of a member of the ICT staff. You must never attempt to use any of the connectors on the back of any desktop computer. You may use USB memory stick ports, floppy disk and CD ROM drives where provided on the front of the computers. You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff.
Portable Devices	Rules governing portable devices – including laptops, iPads and tablets • Portable devices must not be left unattended in a non-secure environment such as an unlocked room. • Portable devices must not be left unattended in a vehicle or public place. • Portable devices may be left unattended in the staff member's place of residence • No-one other than a member of TLE Academy staff may utilise a staff portable device e.g. Family members. • TLE Academy will not be responsible for any unlicensed software which is installed on the portable device. The IT Support Team will never install unlicensed software on such devices. However, staff members are allowed to install licensed or freeware software on the portable devices. • No sensitive data in relation to the business of the academy should be stored locally on the portable device, in line with the Data Protection Act. All data should be stored on the academy server. • If any user has a requirement to store sensitive data locally assistance should be sought from the IT support team to ensure this data is encrypted. • You must not plug any device other than your staff equipment into the network as this presents a significant security, functionality and performance risk. • Confidential information should never be stored on personal computers or portable devices. Only authorised academy based devices and systems should be used to store and transfer confidential information. • Members of staff found to be compromising confidentiality by use of unauthorised devices may be subject to disciplinary action. • Photographs or video images of pupils must only be created using equipment provided by the academy. Members of staff creating or storing images of children using their personal equipment without prior consent may be subject to disciplinary action. Please see the academy's 'E-Safety Policy' for further details.

Virus	Every server, desktop and portable device is installed with an Anti- Virus product. Updates to this software are automatic when connected the academy network. You must not knowingly introduce a virus or carry out any hacking activities. If you suspect that your computer has a virus, you must report it to a member of the ICT staff immediately. If, for any reason, you think that the anti-virus software is not functioning, updating or is not installed then please see a member of the IT support team. You must not: • Remove the anti-virus software or remote update client from any computer • Install additional anti-virus software on any computer • Install any other anti-virus software on your laptop.
Installation of software, files or media	The purchase of software should not be made without consultation with the IT Support team. Staff (with the exception of the IT Support team) must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of the academy's system. The IT Support team will install software for the user or department within the confines of the license agreement. If any user discovers software on a desktop or portable device which he/ she feels is not licensed then they should alert the IT Support team immediately. Software must not be duplicated or distributed outside the scope of its license agreement. Applications used for P2P file sharing such as Kazaa or Bit Torrent, must not be installed on any PC or portable device.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require. If you believe that you have a real need for additional space, please discuss this with a senior member of the ICT support staff.
Transferring files	You may transfer files to and from your network home directories using removable devices. When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so.

	Always check the conditions of use for any electronic material or web site.
Reporting faults and malfunctions	You must report any faults or malfunctions in writing to the ICT support staff including full details and all error messages as soon as possible.
Food and drink	You must not eat or drink nor bring food or drink, including sweets and chewing gum, whilst using the computer. You must maintain a clean and quiet working environment at all times.
Copying and plagiarising	You must not plagiarize or copy any material which does not belong to you.
Copies of important work	It is your responsibility to keep paper copies and back-up copies on the network. TLE Academy will not be responsible for recovering any data which is stored either locally and either corrupted or lost, however will endeavor to recover it wherever possible.
Personal Use	Personal email or internet use must be kept to a minimum such that it does not interfere with the performance of your duties. Legitimate private interests may be followed, providing academy use is not compromised (such interests include private research, work for examination) TLE Academy ICT facilities must not be used for business purposes other than those of TLE Academy. TLE Academy ICT systems must not be disclosed to anyone who is not a direct employee of TLEAcademy. Use of TLE Academy equipment such as computers, phones and/ or tablets to access social networking sites for personal reasons is only acceptable before or after working hours or during break/ lunchtime. Any equipment provided to a member of staff is provided for their personal use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.
Wireless Access	Staff laptops are specifically configured not to allow a connection for anyone other than staff members or members of the IT support team. Wireless connections will not function in most cases when you are logged on locally i.e. logged on to the laptop and not logged on to the TLE Academy network. This is by design to prevent any security breach if a laptop is compromised or stolen.

	No user should attempt to move or reconfigure a wireless network access point. No user should add an additional wireless network access point to the existing wired network. No network cables may be removed or plugged into any device other than to attach a portable device to the network.
Loss or damage to assets	It is the user's responsibility to inform a member of SLT immediately if any computer facilities/hardware or portable devices including I-pads, laptops, phone or tablets become lost, damaged or stolen. After investigation if the damage is a result of negligence individual members of staff may be charged
Ownership and Return of Property	All computing facilities within the academy with the exception of equipment owned personally by staff members are the sole property of the TLE Academy. Any change of ownership must be formally authorised by the governors and management team. All devices must be returned on request to TLE Academy. Devices must be returned with all related accessories, cables and packaging in good working order. If any items are not returned or are not deemed to be in a good working order, you are liable to pay the cost of replacement or repair.

Section Two – Internet Policy and Code of Practice

Introduction

The academy is able to provide access to the internet from desktop PC's via the computer network and through a variety of electronic devices connected wirelessly to the network. Whenever accessing the internet using the academy's or your personal equipment you must observe the code of practice below. This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and the academy's facilities and information being damaged.

Consequently any breach of this policy and the code of practice will be treated extremely seriously and it may result in disciplinary or legal action or expulsion. The academy may take steps, including legal action where appropriate, to recover from an individual any expense or liabilities the academy incurs as a result of the breach of this policy and code of practice by you.

Why is internet access available ?

The internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be useful for educational purposes.

Why is a code of practice necessary ?

There are four main issues:

- Although the internet is often described as 'free', in fact there is a significant cost to the academy for using it. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from ICT staff.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect the Trust's staff and the pupils that access to this unregulated resource is properly managed by the Trust. Accessing certain websites and services and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the academy's network, or passing viruses to a third party, via material downloaded from or received via the internet, or bought into the academy on disk or other storage media.

Code of practice

Use of the internet	The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the internet for other purposes provided that: • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties and • You follow the code of practice at all times. The academy will not be liable under any circumstances for any injury, distress, loss or damage to staff, pupils or parents, which may arise directly or indirectly from the use of Internet facilities, the use of email or from other person's unauthorised use of those facilities or email.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be considered to be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by academy children. **You are responsible for rejecting any links to such material which may appear inadvertently during research.** If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service you must inform the ICT support staff immediately. Please also see the academy's 'E-Safety Policy'.
Web blogs and web publishing.	The rules detailed in Section 3 below are also applicable to web logs or blogs and web publishing. Using images of children for publicity purposes requires the age appropriate consent of the individual concerned and their legal guardians. Images should not be published on websites or in publications without the appropriate consent. Please the academy's 'E-Safety Policy' for further information.
Misuse, abuse and access restrictions	You must not misuse or abuse any website or service, or attempt to bypass any access controls or restrictions on any website or service. Access to some websites is blocked by TLE Academy. If you have a genuine reason to access a blocked website please see a member of the IT Support Team. No unauthorised contract, purchase or payment should be made over

	the Internet. Use for personal financial gain, gambling, political purposes or advertising is forbidden. Permission must be sought from pupils and parents before any personal data i.e. names and photographs are published on website. Please see the academy's 'E-Safety Policy' for further information.
Monitoring	The internet access system used by the academy maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.
Giving out information	You must not give any information concerning the academy, its pupils or parents or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people, the only exception being the use of the academy's name and your name when accessing a service which the academy subscribes to.
Personal safety	You should take care with whom you correspond. You should not disclose where you are nor arrange meetings with strangers you have got in contact with over the internet.
Hardware and software	You must not make any changes to any of the academy's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the academy are an important part of the academy's security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the academy's systems.
Copyright & Intellectual Property	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so. Intellectual property rights must be respected.
Social contact with Pupils (current and former)	Internet, email and approved contact details should be the only means used by members of staff to contact pupils, children or young people. Staff should not give their personal details such as home or phone number, Instant Messenger identities. personal email address or any other unapproved method to pupils. Please see the academy's 'E-Safety Policy' for further information.

Cyberbullying	All forms of bullying, including cyberbullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any user to behave in a manner which is intimidating, threatening or in any way discriminatory. If an allegation is received that a user is responsible for comments made on line which could be deemed harmful, threatening , defamatory abusive or harassing in any way towards another employee, the academy will investigate this matter, Staff should not retaliate to any such incident and should report it as soon as possible to senior management. Please see the academy's 'E-Safety Policy' for further information.

Section Three - E-mail policy and code of practice

Introduction

The academy's computer system enables members of the academy to communicate by e-mail with any individual or organisation with e-mail facilities throughout the world.

For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of e-mail by all.

Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion. The academy may take steps, including legal action where appropriate, to recover from an individual any expense or liabilities the academy incurs as a result of the breach of this policy and code of practice by you.

Code of practice

Purpose	You should only use the academy's e-mail system for academy related emails. You are permitted only to send a reasonable number of e-mails.
Trust's disclaimer	The academy''s e-mail disclaimer is automatically attached to all outgoing e-mails and you must not cancel or disapply it.
Monitoring	Copies of all incoming and outgoing e-mails, together with details of their duration and destinations are stored centrally (in electronic form). **The frequency and content of incoming and outgoing external e-mails are checked from time to time** to determine whether the e-mail system is being used in accordance with this policy and code of practice. The Headteacher, senior staff and technical staff are entitled to have read-only access to your e-mails.

Security	As with anything else sent over the internet, e-mail is not completely secure. There is no proof of receipt, e-mails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, you have to make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by e-mail. Care should be taken with the storage of confidential information. Confidential information should never be distributed through personal email. Members of staff found to be compromising confidentiality by use of personal email may be subject to disciplinary action.
Program files and non-business documents	You must not introduce program files or non-business documents from outside onto the academy's network. This might happen by opening an e-mail attachment or by downloading a file from a web site. Although virus detection software is installed, it can never be guaranteed 100% successful, so introducing nonessential software is an unacceptable risk for the academy. If you have any reason for suspecting that a virus may have entered the academy's system, you must contact the ICT support staff immediately.
Quality	E-mails constitute records of the academy and are subject to the same rules, care and checks as other written communications sent by the academy, so, for example: • You should always consider whether it is appropriate for material to be sent to third parties; • they may have to be disclosed in legal proceedings; • they may have to be disclosed to a person if he makes a request to see information held about him under data protection law; • they require the same level of authorisation before being sent; • printed copies of e-mails need to be retained in the same way as other correspondence; • they are confidential to the sender and recipient, unless you have been given permission to read them; • transmitting the works of others, without their permission, may infringe copyright; • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libellous, malicious, threatening or contravening discrimination legislation or detrimental to the academy is a disciplinary offence and may also be a legal offence. This also includes postings on discussion boards and forums.

Inappropriate e-mails or attachments	You must not use e-mail to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. You must not send personal or inappropriate information by e-mail about yourself, other members of staff, pupils or other members of the academy community. Never open an email and / or attachment from an unsolicited source. Never open an attachment from an unsolicited source or a trusted source if it seems in any way suspicious or non-work related. If you receive any inappropriate e-mails or attachments you must report them to technical staff.
Viruses	If you suspect that an e-mail has a virus attached to it, you must inform the technical staff immediately.
Spam	You must not send spam (sending the same message to multiple e-mail addresses) without the permission of senior staff.
Storage	Old e-mails may be deleted from the academy's server after 12 months. You are advised to regularly delete material you no longer require and to archive material that you wish to keep.
Message size	Staff are limited to sending messages with attachments which are up to 10Mb in size. If you wish to distribute files within the academy, you can do so by using shared areas.
Confidential Emails	You must ensure that confidential emails are suitably protected at all times. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be encrypted before sending and deleted when no longer required.
Social contact with Pupils (current and former)	The provisions outlined above in Section two also apply to email contact. Contact through personal email addresses is not permitted and personal email addresses must not be issued to pupils. Please see the academy's E-Safety Policy, available on 'm'-drive for further information. Also Section 4 below regarding Social Media

E-MAIL POLICY – advice to staff

Staff should remind themselves of the ICT AUP which relates to the monitoring, security and quality of e-mails. In addition staff should be guided by the following good practice:

1. Staff should check their e-mails on a daily basis and respond, as appropriate, within a reasonable period if the e-mail is directly addressed to them

2. Staff should avoid Spam, as outlined in the AUP. Staff should avoid using the e-mail system as a message board and thus avoid sending trivial global messages. Whilst accepting the convenience of the whole staff and teaching staff distribution lists staff should try to restrict its use to important or urgent matters.
3. When global distribution is used, staff should be as specific as possible in the title to so as to alert staff of the content and relevance of the e-mail.
4. Staff should send e-mails to the minimum number of recipients
5. Staff are advised to create their own distribution lists, as convenient and appropriate
6. Staff should always include a Subject line
7. Staff are advised to keep old e-mails for the minimum time necessary

Further guidelines:

1. Remember - E-mails remain a written record and can be forwarded to others or printed for formal use
2. As a rule of thumb staff should be well advised to only write what they would say face to face, and should avoid the temptation to respond to an incident or message by e-mail in an uncharacteristic and potentially aggressive fashion. Remember “tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
3. Remember that sending email from your academy account is similar to sending a letter on academy letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the academy, its business, employee, suppliers or anybody linked to TLE Academy.
4. Do not create or send communications which are defamatory or derogatory.
5. Never send sensitive or confidential information – unless appropriate password protection is applied.
6. Do not create communications which are intimidating, hostile or offensive in any way.
7. Copyright law also applies to all communications.
8. Linked with this, and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

Section Four – Social Media Use –code of practice for staff

1. Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents.

2. Members of staff must not have contact with any pupils, through sites and staff must not add pupils, children or young people or parents as ‘friends’ or respond to friend requests from children if asked on social media sites. If a member of staff suspects than an existing friend is a former or current student, they should report this matter to a member of the SLT immediately.

3. It is recognised that personal access to Social Networking sites outside the work environment is at the discretion of the individual however members of staff and associate workers should consider their use of social networks as they take on the

responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.

4. Secure and suitable strength passwords should be devised and security settings should be applied so access to your profile and the information contained is limited to those explicitly given access.

5. Personal profiles on social networking sites and other internet posting forums must not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, information which is confidential or could put others at risk should not be posted on such public domains. If the material you post or display is considered inappropriate or could be considered to bring the academy or profession into disrepute, disciplinary action may be considered.

Please complete and return the signature sheet at the back of this document to the School Business Manager

TLE Academy

Name:	
Department/Team:	

I confirm I have received a copy of 'Information and Communication Technology Acceptable Use Policy' and that I have read this and understood the contents.

I also confirm that I have sought clarification from my line manager on any issues outlined in this policy which I am not clear about.

Signed: _____

Date: _____

……