IT Services

e-Safety Policy

Document title:	e-Safety Policy
Version number:	1.4
Policy Status	Approved
Date of Issue	May 2016
Date to be revised	May 2017

Revision Log (last 5 changes)

Date	Version No	Brief detail of change
Jan 15	1.0	Initial document for review
Mar 15	1.1	Added appendix
Mar 15	1.2	Added managing risk
Mar 15	1.3	NW changes
May 16	1.4	Reviewed for clarity and reformatted

Contents

This policy applies to all internet, intranet, e-mail and messaging systems and all related technology services provided by LAT, and to all LAT users accessing these services.

This policy is designed to express LAT philosophy with regard to the internet, intranet and electronic communication in general and to set forth general principles that users should apply when using these services whilst at LAT. This guidance does not attempt to cover every possible situation.

This policy has been agreed by the LAT Executive and Academy Senior Management and ratified by the LAT Board. It will be reviewed every twelve months. This policy is maintained by the LAT IT Services Department. Requests to change the policy should be made to the Director of IT Services. All changes will need to be approved by the Trust Executive Group.

1. Introduction

The internet, intranet, e-mail, messaging systems, mobile devices and related technologies can be extremely valuable tools in an educational context, encouraging the development of communication skills and transforming the learning process by opening up possibilities that, conventionally, would be inaccessible.

Creating a safe ICT learning environment within LAT includes four main elements:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- Access to e-safety information for students, staff, parents, carers and other users;
- A commitment to quality e-safety education for all age groups across the academy.

2. Scope

E-safety is seen by LAT as an extension of safeguarding policies and procedures.We aim, therefore, to create a whole-site awareness of the responsibilities, policies and procedures around child safety. Safeguarding users is everyone's responsibility, so these regulations apply to all users, no matter what their responsibilities.

The 'staying safe' outcome encompasses the aims that children and young people are to be:

- safe from maltreatment, neglect, violence or sexual exploitation;
- safe from accidental injury and death;
- safe from bullying and discrimination;
- safe from crime and anti-social behaviour in and out of the academy;
- secure, stable and cared for;
- able to access age-appropriate information, images and video material.

These aims apply equally to the virtual world that children and young people will encounter whenever they use ICT in its various forms.

This policy provides users with guidelines for safe, responsible behaviour whilst accessing Trust systems and the internet. Please refer to the LAT IT Security Policy for guidance regarding the security of data and IT equipment.

3. Technology

ICT in the 21st century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used at LAT and, more importantly in many cases, outside LAT by children include:

- The internet;
- E-mail and webmail - e.g. www.hotmail.co.uk and www.yahoo.co.uk;
- Instant messaging, often using simple web cams - e.g. www.msn.com and www.aim.com;
- Blogs (online interactive diaries) - e.g. www.blogger.com;
- Podcasting (radio / audio broadcasts downloaded to computers or MP3/4 players);
- Social networking sites - e.g. www.myspace.com, www.bebo.com, www.facebook.com and www.twitter.com;
- Video broadcasting sites - e.g. www.youtube.com;
- Chat rooms - e.g. www.teenchat.com and www.habbohotel.co.uk;
- Gaming sites - e.g. www.neopets.com, www.miniclip.com/games/en and www.runescape.com;
- Music download sites - e.g. www.napster.co.uk, www.kazzaa.com and www.limewire.com;
- Mobile phones with Bluetooth, messaging, camera and video functionality;
- Messaging or Bluetooth communications between systems and mobile devices;
- Smartphones with e-mail, web functionality and limited 'Office' applications;
- Mobile devices with internet access, both inside and outside LAT;
- Remote access to a LAT network;
- LAT-provided systems, such as the intranet and learning platforms.

4. Statement of Responsibilities

LAT has a responsibility to ensure that all reasonable and appropriate steps have been taken to protect users whilst using technology.

Responsibilities of staff include the following:

- Although all staff have a responsibility to exercise a duty of care, it is important that staff are aware of their specific obligations with regard to e-safety;
- All staff are responsible for their own actions and the use of IT facilities whilst conducting their work. LAT assumes and implies compliance with this policy, without exception;
- All staff should be familiar with current policies, standards and legislation relating to the use of the internet;
- All staff should comply with the security measures laid down in this policy. Abuse of the computer network or the internet may result in disciplinary action, including possible termination of employment and civil and / or criminal liability;

- All staff should ensure they know how this policy relates to all other related LAT or Academy policies e.g. Anti Bullying and the implications of the use of IT in their classes.
- The person responsible for the e-Safety of students at each academy should also have responsibility, together with the Trust Director of IT, to review e-Safety in the Academy on a regular basis, at least twice every academic year.

Responsibilities of the academy leadership team, in liaison with the Trust's IT team at their academy, include:

- Distributing the e-Safety Policy to all staff;
- Ensuring that all staff are aware of the policy;
- Maintaining e-safety procedures appropriate to the information systems in use;
- Keeping accurate records of all staff and students who are granted internet access. These records will be kept up to date, taking account of events such as staff leaving LAT or the withdrawal of a student's access;
- Ensuring all inappropriate use of technology is dealt with and its occurrence is monitored.

Responsibilities of the IT Services team include:

- The development of the LAT E-Safety Policy;
- Reviewing this policy regularly in the light of ever-changing technologies;
- Providing the necessary software tools and security utilities to maintain the integrity and confidentiality of the academy's systems - e.g. use of up-to-date virus-scanning software;
- Ensuring security systems, firewalls and virus-scanning software (where appropriate) are up to date.

5. Misuse

The internet, intranet, email, messaging systems and related technologies must not be used for knowingly viewing, communicating, retrieving, downloading or storing any communication that is:

- Discriminatory or intended to harrass;
- Derogatory to any individual or group;
- Obscene or pornographic;
- Defamatory, threatening or capable of being construed as cyber-bullying;
- Illegal or contrary to LAT's policy or interests;
- Subject to copyright, as is the case with music, software and films;
- Likely to cause network congestion or significantly hamper access by other users;
- Any of the above, especially using mobile devices or similar technologies to store or upload any such materials to the public domain (social networking sites) or to other devices.

Except in cases in which explicit authorisation has been granted by the LAT Executive team, users are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other users;
- Using other users' log-in details or passwords;
- Breaching, testing or monitoring computer- or network-security measures;

- E-mail or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else;
- Hacking, Bluejacking or accessing systems or accounts that they are not authorised to use;
- Obtaining electronic access to other companies' or individuals' materials. (Copyright prohibits users from copying, retrieving, modifying or forwarding copyright materials, except as permitted by the copyright owner).

Law and LAT policy prohibits the theft or abuse of computing resources and includes:

- Unauthorised entry;
- Using, transferring and tampering with other people's accounts and files;
- Interfering with other people's work or computing facilities;
- Sending, storing or printing offensive or obscene material, including content that may be interpreted as sexual or racial harassment;
- Mass mailing of messages;
- Internet use for personal commercial purposes;
- Using the internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations;
- Accessing or uploading information to any obscene or pornographic sites. Sexually-explicit material may not be viewed, archived, stored, distributed, edited or recorded using the academy's networks or computing resources.

If a user finds himself/herself connected accidentally to a site that contains sexually explicit or offensive material, s/he must disconnect from that site immediately. Such unintentional access to inappropriate Internet sites must be reported immediately to the respective tutor, line manager or principal. Any failure to report such access may result in disciplinary action.

It is impossible to define all possible unauthorised use. However, disciplinary action may be taken where a user's actions warrant this. Other actions deemed unacceptable include, but are not limited to:

- Theft or copying of files without permission;
- Sending or posting LAT's or other stakeholders' confidential files, whether outside the organisation or to unauthorised staff, students or other users inside LAT;
- Refusing to co-operate with reasonable security investigations.

6. Passwords

With the advent of increasingly sophisticated password-cracking programmes, steps need to be taken to minimise the problem posed by malicious users trying to break into accounts. The security of passwords used with accounts is a highly-important issue. The passwords you use should be carefully considered, as badly-chosen passwords have the potential to be cracked or easily guessed. The following principles should be followed:

- Passwords must be at least eight characters long and should be a combination of letters and numbers;
- A password must not be based on anything connected with the individual who owns the account. This includes anything associated with a name, initials, job description, address or postcode;
- Any password generated for use by the IT Services team should be changed immediately after initial use;
- User accounts are issued by the Trust's IT team for individual use only;
- Accounts and passwords must not be shared, given away or offered for use to anybody else;
- Users must take all reasonable steps to keep their passwords confidential and must not disclose them to anyone else;
- Passwords should be changed every 60 days.

7. Internet Access

All access to the internet at each academy must take place via the filtering software installed by LAT. This filtering software should help to prevent access to inappropriate sites available over the internet. However, no automatic filtering service can be 100% effective in preventing access to such sites and it is possible that users may accidentally access unsavoury material whilst using the internet. In such circumstances, users must exit the site immediately and advise the person responsible for IT in the academy, providing details of the site, including the web address, to reduce the possibility of the material being accessed again in future. The person responsible for IT will then arrange for the filtering rules to be revised to exclude the site.

Access to the internet is available for authorised users only and is provided to support work-related activities and for educational purposes only.

There is a huge amount of information available to users via the internet and students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students should be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

8. E-mail, Messaging and Social Networking

Those that use LAT's e-mail, messaging or other digital communication services are expected to do so responsibly, to comply with all applicable laws, other policies and procedures of LAT and to observe normal standards of professional and personal courtesy and conduct.

LAT follows sound professional practices to secure e-mail records, messaging systems, data and system programmes under its control. As with standard paper-based mail systems, confidentiality of these cannot be 100% assured. Consequently, users should consider the risks when transmitting highly-confidential or sensitive information and should use the appropriate level of security measure.

Enhancement of base-level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered that messages forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such correspondence.

In order to manage these systems effectively, the following should be observed:

- Open messages/mailboxes must not be left unattended;
- Care should be taken about the content of a message, which has the same standing as a letter;
- A report should be made immediately to IT Services when a virus is suspected in a message.

Users must not:

- Ignore messages. These systems are designed for speedy communication. If the message requires a reply, a response should be sent promptly within reasonable working hours;
- Use anonymous messaging services to conceal their identity when mailing through the internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any internet service which requests name, e-mail address or other details;
- Abuse others, even in response to abuse directed at them;
- Use these technologies, either internally or on the internet, to sexually harass fellow employees, or to harass or threaten anyone in any manner.

The transmission of user names, passwords, chain mail or other information related to the security of the LAT computers is not permitted.

Although not allowed within the academies, we do realise that the majority of young people use social-networking sites at home. We aim to make students responsible users of these sites and students should therefore be made aware of the advantages and dangers of using these websites.

9. Media Publications

Video and photographic technologies can be very powerful learning tools. However, photographs and/or video may be taken by staff to support educational aims only. Named images of students will only be published with the separate written consent of their parents or carers. Publishing includes, but is not limited to:

- LAT websites and newsletters;
- Web broadcasting;
- TV presentation;
- Newspapers.

Care should be taken when capturing photographs or videos to ensure that all students are appropriately dressed and permissions have been obtained from parents and carers in line with normal guidance.

10. Use at Home

Students, staff or other users accessing the internet from home whilst using an LAT-owned computer or mobile device, or through LAT-owned connections such as the remote desktop connection (Citrix Link), must adhere to the policies set out in this document.

Family members and other non-LAT users must not be allowed to access LAT computer systems or use the LAT computer facilities, without the formal agreement of the LAT Executive/principal.

11. Monitoring

Users are given network and internet access to assist them in their role within the Trust and each academy. Users expressly waive any right of privacy and should therefore have no expectation of privacy in anything they create, store, send or receive using LAT computer equipment. The computer network is the property of LAT and may be used only for LAT purposes.

LAT has the right to monitor and log any and all aspects of its computer system including, but not limited to, monitoring internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads and all communication sent and received under the Investigatory Powers Act 2000. Please refer to the regulatory framework section for more information regarding this Act.

Managers will not routinely have access to a user's personal file area. However, usage statistics/management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time.

However, no personal data will be retained unless it is potentially illegal. In such a case, the Trust Executive/principal will manage the information in confidence, in line with the LAT Data Protection Policy, and will discuss the issue with the member of staff concerned. It is the Trust Executive's /Principal's responsibility to decide whether to take any further action. All personal information collected by way of monitoring will be destroyed when it has become redundant.

LAT will utilise software that makes it possible to identify and block access to internet sites containing sexually-explicit or other material deemed inappropriate in the workplace.

12. Managing Risk

We recognise that it is impossible to eliminate e-safety risk, whilst harnessing the power of technology for learning. Each academy is therefore required to complete the e-safety risk register, which is reviewed and updated every six months.

Each academy is required to plan and deliver a training and education programme for all its stakeholders; this is updated and reviewed annually, evaluating its effectiveness in providing the necessary preventative skills.

The e-Safety Officer at each academy is required to be trained by a relevant body on current e-safety issues, legislation and procedures for responding to incidents as they occur. The e-Safety Officer should share important information with all staff regularly and ensure that all understand that there is a collective responsibility for e-safety across the academy. This training should be regularly updated to ensure that each academy is fully aware of changing trends in children's use of technology.

13. Complaints

LAT will take all reasonable precautions to ensure that users are staff when using technology. However, owing to the international scale and interlinked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a LAT computer or mobile device. LAT cannot accept liability for material accessed, or for any consequences of internet access.

Students and staff have access to information about infringements in use and possible sanctions.

In addition to the usual academy sanctions, the following may be appropriate:

- Interview or counselling by an appropriate member of staff;
- Removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including staff files or student examination coursework;
- Referral to social services/police or other authorities.

The Academy e-Safety Co-ordinator acts as first point of contact for any complaint. However, any complaint about misuse by staff, students or other users can also be referred to the principal.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to safeguarding are dealt with in accordance with Trust safeguarding policy and procedures.

14. Regulatory Framework

All users should ensure that they are familiar with the items in the following paragraphs.

14.1 Data Protection Act 1998

The Data Protection Act states that anyone processing personal data must comply with the principles of good practice. These are that the data must be fairly and lawfully processed, accurate, up to date, relevant, not kept for longer than is necessary, secure and processed for limited purposes.

Before any member of staff plans to process and store data about a person, however small the amount, they must check whether notification is needed under the Data Protection Act. Staff should contact the Data Protection Officer responsible for data protection within the academy.

14.2 Copyright, Design and Patents Act 1988 & Copyright and Trade Marks Act 2002

The Copyright, Design and Patents Act's purpose is to protect the ownership rights of authors, designers, inventors, etc. It is relevant to computers as it also protects writers of computer software. It makes it an offence to use unlicensed software (software that has been copied, or where licensing agreements have been contravened).

Software cannot simply be downloaded and used freely. However, free use is often granted under certain conditions, so make sure that these are read and understood - even 'freeware' often has conditions attached. Under no circumstances should software be downloaded from the internet unless you are authorised by management to do so.

The Copyright and Trade Marks Act 2002 is aimed at combating growing piracy and counterfeiting. It strengthens existing laws governing use of software legislation and gives courts stronger powers.

It is therefore essential that LAT should check on the use of software, for three important reasons:

- To ensure that each academy has sufficient licenses, as well as ensuring that they are not paying more in licensing and support fees than necessary,
- To be aware of the software and licenses available to the academy
- To comply with the law.

Failure to comply:
In certain circumstances an organisation, through its officers, faces unlimited fines and/or up to two years' imprisonment if it is convicted of infringing the copyright in software. The same applies to individuals or individuals within organisations. In addition to unlimited fines and convictions, an organisation and its employees risk civil action by software companies seeking damages. Under the Copyright and Trade Marks Act 2002, the maximum penalty for copyright theft was increased from two to ten years for organisations making unauthorised copies of copyright works.

14.3 Computer Misuse Act 1990

The Computer Misuse Act makes it a criminal offence to hack into someone else's computer. A hacker is someone who gains access to a computer without permission, usually for one or more of the following reasons:

- to steal, alter data, or damage the system;
- to show off their technical skills;
- To poke fun (this is the excuse hackers tend to use).

The Act introduces three criminal offences:

- Unauthorised access - this covers accessing other people's computers without their express permission or gaining access to data normally denied to you. A person is guilty of an offence if

they cause a computer to perform any function with the aim of gaining unauthorised access to any programme or data held on any computer;

- Unauthorised access with intent to commit a further serious offence - for example, in cases where a hacker gains access to a security system with the intention of carrying out a burglary. The burglary does not need to have taken place;
- Unauthorised modification of computer material - this includes gaining unauthorised access and making changes to data; introducing a virus into a computer system; and any unauthorised change to a system, including introducing programmes with intent to disrupt and destroy data held on a computer system. 'Unauthorised access' is access of any kind by any person to any programme or data held in a computer, if:

a. That person is not entitled to access the programme or data;
b. That person does not have consent to access the programme or data from any person who is entitled to authorise access.

You would therefore be committing a criminal offence by gaining access to an unattended computer or mobile device which is, at the time, logged into a network or system that you are not entitled to use or access, or by using a password other than one belonging to you to gain access to programmes or data that you are not entitled to use.

To prove that an offence has taken place, you must be able to demonstrate that the hacker:

- Deliberately accessed the system;
- Was not authorised to access the system;
- Knew at the time what he or she was doing.

14.4 The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers makes it legal for employers and others in a position of authority to monitor and analyse transactions taking place in an organisation using the organisation's resources. This particularly applies to e-mails which are sent and received using the organisation's resources. These e-mails represent the organisation and are, therefore, subject to the organisation's rules and procedures.

This act permits LAT to vet communications without the consent of the caller, writer or recipient, where the intention is:

- to establish the existence of facts applicable to LAT;
- to ascertain compliance with regulatory practices;
- for the purposes of quality control;
- to detect viruses or other dangers to the system;
- to determine whether communications are relevant to LAT.

14.5 Lawful Business Practice (LBP) Regulations

The LBP Regulations authorise employers to monitor or record communications without consent for a number of purposes, including the following:

- To establish the existence of facts relevant to the business;
- To ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business;
- To ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system;
- To prevent or detect crime;
- To investigate or detect the unauthorised use of telecommunication systems.

The Regulations cover all types of communications, including those that are internet-based, or carried out by fax or e-mail.

15. Appendix

Leigh Academies Trust IT Acceptable Use Policy

Leigh Academies Trust (LAT) are committed to making full use of appropriate ICT resources and new technologies to make learning as exciting, interesting and relevant as possible.

It is acknowledged that with new technologies, such as the internet, there are risks to students relating to accessing inappropriate content, receiving unwanted attention or being vulnerable to cyber-bullying. The Trust believes it is our responsibility to educate students to ensure that they are well aware of the dangers in order to maximise the safe use of ICT.

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this Acceptable Use Policy as part of their contract of employment. Members of staff should consult the LAT e-Safety Policy for further information and clarification.

For reference, ‘user’ refers to any authorised user or employee of the Trust.

When using ICT at an academy:

IT hardware must be treated with care and used only in accordance with the proper operating instructions. No equipment shall be used which is labelled as out of order. Any apparent fault with hardware should be reported promptly to the IT Services Helpdesk. Equipment must not be used if there is reason to believe that it may not be in safe working order.

Users must not, by any deliberate or careless act or omission, jeopardise or seek to jeopardise the integrity of any IT equipment and/or its software and/or any information stored within it and/or accessed through it.

Users must not access and/or attempt to access any IT equipment, software and/or data that they are not properly authorised to access. In particular, the confidentiality of data belonging to other users must be respected.

Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage areas and/or passwords allocated for their use. Users must not use access codes that belong to someone else; give out passwords to unauthorised persons, allow others access using their username or aid anyone to enter the system, except by authorised means.

Users must not use any IT facility for a purpose other than that for which they are authorised. Users must seek advice if they have any doubt about their authority to use any of the IT facilities.

Users must comply with all their legal obligations affecting their use of IT facilities, including contempt of court, copyright, defamation, the Computer Misuse Act, the Data Protection Act, the Official Secrets Act, the Obscene Publications Act, the Protection of Children Act and the Equality Act.

Users must take all reasonable steps to exclude and avoid the spread of malicious software - e.g. viruses - and must co-operate fully with all measures instituted by IT Services to prevent the spread of such software. In particular, users must not install or execute on a LAT computer any software obtained from a third-party source. Under the Computer Misuse Act 1990, it is an offence knowingly to corrupt a computer programme or any of the data stored in the computer system.

Computer programmes on IT facilities are protected by the law of copyright. LAT has the appropriate licences to use these programmes. Users must comply with all their legal obligations concerning copyright and must not copy any software or other data without prior authorisation from the copyright owner. Such action would be in breach of copyright law.

Users must not connect any unauthorised equipment to LAT networks without consultation and the prior written approval of a senior member of the IT Services Department. If IT Services has reasonable grounds for believing that any equipment may be the cause of unacceptable degradation of the performance of the network and detrimental to other users, then the user must co-operate with the disconnection of the equipment from the network pending resolution of the problem.

The use of any IT equipment for storage and/or transmission of materials which LAT considers to be obscene and/or offensive is strictly prohibited

Users must understand that students are not permitted to use their devices and will ensure they are logged out before leaving any device unattended, and securely locked away when they are not being used

Users must be aware of their responsibilities for the safe printing and collection of sensitive information.

When using the internet:

Users must be aware that the Trust cannot accept any responsibility for personally downloaded content or software;

Users must understand that under no circumstances should attempts be made to bypass the internet-filtering system, as it exists to safeguard both staff and students;

Users should understand that the use of the Trust's information systems, internet and e-mail may be monitored and recorded to ensure policy compliance;

Users must not send staff or students personal information via the internet without authorisation from their line manager;

Users must understand that, when using social-networking sites for personal use, the user will not contact or communicate with students or parents;

Users must ensure that electronic communications with students, including e-mail, IM and social networking, are compatible with the user's professional role and that messages cannot be misunderstood or misinterpreted;

Users must promote e-safety with students and will help them to develop a responsible attitude to system use, communications and publishing;

Users must not use IT facilities to download pornographic, obscene, excessively violent and/or offensive materials from the internet.

LAT may exercise its right to monitor the use of academy information systems and Iinternet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the academy's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

LAT views the unauthorised access or interference with any of its IT facilities as an extremely serious disciplinary offence. Any breach of these regulations shall be dealt with in accordance with the disciplinary procedures of LAT, as applicable to the user concerned. In the case of a serious breach, the authorisation of a user to use particular IT facilities may be withdrawn immediately on the instruction of a member of the Trust Executive and/or academy senior leadership team.

IT Services may revise or modify this policy without prior notification. To view current policy information, please check the staff portal.

I have read, understood and accept the LAT Staff Acceptable Use Policy.

Name: Signed: Date: