IT Services

Online Safety Policy

Document title:	Online Safety Policy
Version number:	1.7
Policy Status	Approved
Date of Last Review	December 2019
Date to be revised	December 2020

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
June 17	1.5	Reviewed and updated

September 2018	1.6	Reviewed and updated, typos and removal of unrelated data. GDPR update
December 2019	1.7	Reviewed and updated

Contents

This policy applies to all Internet, Intranet, e-mail, 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 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 LAT Executive, 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 impossible to achieve.

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 and carers and other users;
- A commitment to quality e-Safety education at all age groups across the academy

2. Scope

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

The 'staying safe' outcome includes aims that children and young people are:
● safe from maltreatment, neglect, violence and sexual exploitation;
● safe from accidental injury and death;
● safe from bullying and discrimination;
● safe from crime and anti-social behaviour in and out of Academy;
● secure, stable and cared for;
● are 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 gives users guidelines for safe, responsible behaviour whilst accessing the 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, used outside of LAT by children include:

- The Internet
- E-mail and Webmail e.g. www.hotmail.co.uk, www.yahoo.co.uk;
- Instant messaging often using simple web cams e.g. www.msn.com, www.aim.com; www.whatsapp.com
- Blogs (an on-line interactive diary) e.g. www.blogger.com;
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
- Social networking sites e.g. www.myspace.com, www.bebo.com, www.facebook.com; www.twitter.com;
- Video broadcasting sites e.g. www.youtube.com;
- Chat Rooms e.g. www.teenchat.com, www.habbohotel.co.uk;
- Gaming Sites e.g. www.neopets.com, www.miniclip.com/games/en, www.runescape.com;
- Music download sites e.g. www.napster.co.uk, www.kazzaa.com, www.limewire.com;
- Mobile phones with, Bluetooth, messaging, camera and video functionality;
- Messaging or Bluetooth communications between systems and mobile devices;
- Smart phones with e-mail, web functionality and cut down 'Office' applications;
- Mobile devices that access the Internet both inside and outside of 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

- Although all staff have a responsibility to exercise a duty of care, it is important that staffs are aware of their specific obligations with regard to e-Safety.
- All staffs 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 IT team at their Academy:

- Distributing the e-Safety Policy to all staff;
- Ensuring all staff are aware of the Policy;
- Maintaining e-Safety procedures appropriate to the information systems in use;
- Keep accurate records of all staff and students who are granted Internet access. These records will be kept up-to-date, with such as a member of staff leaving or the withdrawal of a student's access.
- Ensuring all inappropriate use of technology is dealt with and their occurrence is monitored.

Responsibilities of the IT Services Team:

- The development of the LAT E-Safety Policy.
- To review 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 systems e.g. use of up to date virus scanning software
- Ensuring security systems, firewalls, 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 harassing;
- Derogatory to any individual or group;
- Obscene or pornographic;
- Defamatory, threatening or seen as cyber bullying;
- Illegal or contrary to LAT policy or interests;
- Subject to Copyright such as music, software or films;
- Likely to cause network congestion or significantly hamper access for other users;
- Any of the above, specifically 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 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 user's log-ins 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, Blue-jacking or accessing systems or accounts that they are not authorised to use;
- Obtaining electronic access to other companies' or individuals' materials. (Copyright means users cannot copy, retrieve, modify or forward copyrighted 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 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, they 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 warrants it. Other actions deemed unacceptable, although not exhaustive, include:

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

6. Passwords

With the advent of increasingly sophisticated password cracking programs, 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.

- Passwords must be at least 8 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 or initials, job description, address or postcode.

- Any passwords generated for use by the IT Services Team should be changed immediately after initial use.
- User accounts are issued by the Trust 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 be 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. Email, Messaging and Social Networking

Those that use the LAT e-mail, messaging or other digital communication services are expected to do so responsibly, comply with all applicable laws, other policies and procedures of LAT and with 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 use the appropriate level of security measure.

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

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

- Open messages/mailboxes must not be left unattended;
- Care should be taken about the content of a message as it has the same standing as a letter;
- Report 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 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 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 are using social networking sites at home. We aim to make students responsible users of these sites and therefore students should 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 presentations
- Newspapers

Care should be taken when capturing photographs or videos to ensure that all students are appropriately dressed and permissions gained 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 (Duo Link) must adhere to the policies set out in this document.

Family members or other 'non-LAT' users must not be allowed to access LAT computer systems or use the LAT computer facilities.

11. Monitoring

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

The 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 there is any potential illegality. In such a case the Trust Executive/Principal will manage the information in confidence, in line with the LAT Data Protection Policy and discuss the issue with the member of staff concerned. It is the Trust Executive/Principal's responsibility to make the decision 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. Therefore each academy is required to complete the e-Safety risk register, which is reviewed and updated every 6 months.

Each academy is required to plan and deliver a training and education program 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 all understand that there is a collective responsibility for e-Safety across the Academy. This training should be regularly updated to ensure each academy is fully aware of changing trends in children's use of technology.

13. Complaints

LAT will take all reasonable precautions to ensure users are staff when using technology. However, owing to the international scale and linked 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 any consequences of Internet access.

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

In addition to usual Academy sanctions the following may be appropriate:

- Interview or counselling by 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 Coordinator acts as first point of contact for any complaint. However, any complaint about staff, student or other users misuse 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 following items:

14.1 Data Protection Act 2018

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Before any member of staff plans to process and store data about a person, however small the amount, they must contact the Local Data Officer (LDO) responsible for Data Protection within the Academy. Any data processing are dealt with in accordance with our Data protection policy.

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 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.

Therefore it is essential that LAT 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 what software and licenses are 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 in software. Under the Copyright and Trade Marks Act 2002 the maximum penalty for copyright theft increases from two to ten years for organisations making unauthorised copies of copyrighted 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;
- 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 to receive unauthorised access to any program or data held on any computer;
- Unauthorised access with intent to commit a further serious offence - for example 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 to a computer system; and any unauthorised change to a system - introducing programs with the intent to disrupt and destroy data held on a computer system. 'Unauthorised Access' is access of any kind by any person to any program or data held in a computer is unauthorised if:

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

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

To prove 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 emails which are sent and received using the organisation's resources. These emails 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 Regulations (LBP)

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, by fax and by email.