LIPA SIXTH FORM COLLEGE

E-Safety Policy

Version Date:	August 2018
Document Owner:	Charles Bartholomew, Headteacher
Next Review Date:	August 2020
Approving Committee	Governing Board

Document Version History

Version	Date	Ref	Change Summary
1.0			New Policy.
1.1	August 2018		Reviewed.

E-Safety Policy

Our Vision for E-Safety and why Internet use is important

- LIPA Sixth Form College provides a diverse, balanced and relevant approach to the use of technology
- Learners are encouraged to maximise the benefits and opportunities that technology has to offer
- LIPA Sixth Form College ensures that Learners study in an environment where security measures are balanced appropriately with the need to learn effectively
- We aim to equip Learners with the skills and knowledge to use technology appropriately and responsibly
- LIPA Sixth Form College teaches how to recognise the risks associated with technology and how to deal with them, both within and outside the college environment
- We believe that all users in our college community understand why there is a need for an ESafety Policy
- The purpose of Internet use in college is to raise educational standards, to promote learner achievement, to support the professional work of staff and to enhance the college's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is a part of everyday life for education, business and social interaction. The college has a duty to provide students with quality Internet access as part of their learning experience.
- Learners use the Internet widely outside college and need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

- It aids the exchange of curriculum and administration data;
- It gives access to world-wide educational resources including museums and art galleries;
- It allows educational and cultural exchanges between learners world-wide;
- For vocational, social and leisure use in libraries, clubs and at home;
- It gives access to experts in many fields for learners and staff;
- It facilitates professional development for staff through access to national developments, educational materials and effective curriculum practice;
- It allows collaboration across networks of colleges, support services and professional associations;

- There is improved access to technical support including remote management of networks and automatic system updates;
- It gives access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The college will ensure that the copying and subsequent use of Internet derived materials by staff and learners complies with copyright law.
- Learners will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Access levels will be reviewed to reflect the curriculum requirements and age of learners.
- Staff should guide learners to on-line activities that will support the learning outcomes planned for the learners' age and maturity.
- Learners will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Roles and Responsibilities Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Director and Senior Leaders:

- The Director is responsible for ensuring the safety (including e-safety) of members of the college community, though the day-to-day responsibility for E-safety will be delegated to the Designated Safeguarding Lead.
- The Director / Senior Leaders are responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Director / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in college who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Director should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of a well-planned curriculum and a necessary tool for staff and learners, and so the college has a duty to provide learners with quality Internet access as part of their learning experience:

- The college Internet access will be designed expressly for learner use including appropriate content filtering, including keeping learners safe from terrorist and extremist material whilst accessing the internet.
- Learners will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Learners will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The college will ensure that the use of Internet derived materials by staff and learners complies with copyright law.
- When Learners are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning

How will information systems security be maintained?

- Virus protection will be updated regularly.
- The security of the college information systems and users will be reviewed regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved software will not be allowed in learners' work areas or attached to email.
- Files held on the college's network will be regularly checked.
- The ICT co-ordinator / network manager will review system capacity regularly.
- The college Internet access will be designed to enhance and extend education.
- Learners will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- In line with the requirements of the Data Protection Act (1998), sensitive or personal data is: recorded, processed, transferred and made available for access in college. This data must be: Accurate, Secure, Fairly and lawfully processed, Processed for limited purposes, Processed in accordance with the data subject's rights, Adequate, relevant and not excessive, kept no longer than is necessary, only transferred to others with adequate protection.
- All data in LIPA Sixth Form College is kept secure and staff informed of what they can or can't do with data through the E-Safety Policy and statements in the

Acceptable Use Policy (AUP). Digital data is password protected. Only the HT has access to all passwords. There are various levels of passwords for different users.

- The Director is responsible for managing information
- Staff know the location of data relevant to them
- Staff with access to personal data understand their legal responsibilities with reference to confidentiality, and if they are unsure in a certain area, they know to always be cautious and check with Director before releasing any data.
- All sensitive data is to be stored on the College servers in password protected areas. Extremely sensitive data is in one place where only two people have security access.
- Staff are aware that they should only use approved means to access, store and dispose of confidential data.
- Staff do not have remote access to college data.
- Personal removable USB drives and SD cards should not be used in College, however, if there is no other way, the device needs scanning by HT first.

How will e-mail be managed?

- Learners may only use approved e-mail accounts.
- Learners must immediately tell a teacher if they receive offensive e-mail.
- Learners must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on college headed paper.
- The forwarding of chain messages is not permitted.

- Staff should not use personal e-mail accounts during college hours or for professional purposes.
- All College E-mails contain an appropriate disclaimer

  This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent LIPA Sixth Form College. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both college policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.'

Use of Digital Media

As photographs and video of learners and staff are regarded as personal data in terms of The Data Protection Act (1998), you must have written permission.

- Images of learners are retained indefinitely after they have left College. This is made explicitly to parents/carers in the e-safety/home learning agreement.
- Staff and learners aware that full names and personal details will not be used on any digital media, particularly in association with photographs
- Parents/carers, who have been invited to attend college events, are allowed to take videos and photographs but they are only for use in their home – they are not to be uploaded onto Social Networking Sites. This is made explicitly to parents/carers in the E-safety agreement.
- Staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- We ensure that photographs/videos are only taken using college equipment and only for college purposes
- Staff are allowed to store digital content on personal equipment as long as they understand that the personal equipment must be password protected, and no other users at home are allowed access to the content. Setting up a unique password protected college account on a home PC is allowed.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted

How will published content be managed?

- The contact details on the website should be the college address, email and telephone number.
- Staff or learners' personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT').

- The Director will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the college's guidelines for publications including respect for intellectual property rights and copyright.

Can learners' images or work be published?

- Images that include learners will be selected carefully and will not provide material that could be reused.
- Learners' full names will not be used anywhere on the website, particularly in association with photographs.
- Learners work can only be published with their permission.

How will social networking, social media and personal publishing be managed?

- Teachers are advised not to use any social network space. Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook and Twitter. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old. All staff need to be aware of the following points:
    - The colleges will block/filter access to social networking sites.
    - Newsgroups will be blocked unless a specific use is approved.
    - Learners will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, college attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
    - Personal mobile phones are to be used for security purposes on college activities e.g. college trips

How will filtering be managed?

- The college will work with its ICT Provider and LIPA's ICT Development Team to ensure that systems to protect learners are reviewed and improved.
- If staff or learners discover unsuitable sites, the URL must be reported to the Designated Safeguarding Lead.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

How will video conferencing be managed?

The equipment and network

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Users

- Parents and carers should agree for their Learners to take part in videoconferences, probably in the annual return
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.
- All video conferences must be supervised by a teacher

Content

- Video
- Conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Videoconferencing should be supervised appropriately for the learners' age.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non- college site it is important to check that they are delivering material that is appropriate for your class.
- When recording a video conference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed.
- Mobile phones will not be used during lessons or formal college time (as part of the College AUP). The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a college phone where contact with learners is required.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

How will Internet access be authorised?

- All staff must read and sign the Acceptable Use Policy before using any college ICT resource.
- The college website effectively communicates E-Safety messages to parents/carers
- All website editors are made aware of the guidance for the use of digital media on the website
- All website editors are aware of the guidance regarding personal information on the website
- Only the Marketing Manager has permission to edit the college website
- The Director has overall responsibility for what appears on the website
- Downloadable materials will be provided in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the colleges consent.

How will risks be assessed?

- The college will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a college computer. The college cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The college will audit ICT use to establish if the E–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Acceptable Use Policy (AUP)

- An Acceptable Use Policy is intended to ensure that all users of technology within college will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.
- AUPs are recommended for Staff, Learners and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. A list of Learners who, for whatever reason, are not allowed to access technology must be kept in college and made available to all staff.

Our college AUPS must:

- Be understood by each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the E-Safety Policy/AUP.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
  - ✓ Cyberbullying
  - ✓ Inappropriate use of email, communication technologies and Social Network sites and any online content
  - ✓ Acceptable behaviour when using college equipment /accessing the college network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (this may be linked to your Behaviour Policy).
- Stress the importance of E-Safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

Dealing with Incidents

An incident log is completed to record and monitor offences. This is audited half termly by the Designated Safeguarding Lead or other designated member of the Senior Leadership Team.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Director who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) . They are licensed to investigate – colleges are not!

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in college. Full details are set out in the college's policy on anti-bullying.
- All incidents of cyberbullying reported to the college will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

Learners, staff and parents/carers will be advised to keep a record of the bullying as evidence.

How will Learning Platforms and Learning Environments be managed - Moodle?

- SLT and staff will monitor the usage of the Learning Platform by learners and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Learners/staff will be advised on acceptable conduct and use when using the learning platform.
- Only members of the current learner, parent/carers and staff community will have access to the Learning Platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform.

Infrastructure and technology

Learner access

Learners are always supervised by a trusted adult when accessing college equipment and online materials

Passwords

Staff are aware of the following guidelines concerning passwords:

- Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data involved, e.g. 'master user' passwords are more critical. Users should be instructed on appropriate techniques for selecting and setting a new password.
- Passwords should be changed frequently to previously unused passwords. Many

systems have the capability to prompt or force the user, periodically, to select a new password. The System Manager should decide on the appropriate duration that users could leave their password unchanged. A typical period is termly. The interval chosen and the methods by which the password changes will be enforced must be suitably documented for users.

- A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:
    - when a password holder leaves the college or is transferred to another post;
    - when a password may have become known to a person not entitled to know it.
- The need to change one or more passwords will be determined by the risk of the security breach.
- Users must not reveal their password to anyone. Users who forget their password must request the System Manager issue a new password.
- Where a password to boot a PC or access an internal network is shared, users must take special care to ensure that it is not disclosed to any person who does not require access to the PC or network
- All users of the college network have a secure username and password
- The administrator password for the college network is available to the Director and is kept in a secure place
- Staff and learners are reminded of the importance of keeping passwords secure.
- Staff passwords will be changed each term.
- Staff and learner passwords are combinations of numbers and letters. Administrator passwords are combinations of numbers, letters and special characters.

How will the policy be introduced to learners?

- An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use. All learners and staff are required to read and sign the E-Safety agreement and/or the acceptable use policy. Age appropriate discussions will take place with Learners before the sign the E-Safety Agreement.
- E-Safety rules will be posted in rooms with Internet access.
- An E–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Learner instruction in responsible and safe use should precede Internet access.
- All users will be informed that network and Internet use will be monitored.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum.

Particular attention will be given where learners are considered to be vulnerable.

How will the policy be discussed with staff?

- The E–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct is essential.

- Staff training in safe and responsible Internet use both professionally and personally will be provided.
- To protect all staff and learners, the college will implement Acceptable Use Policies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the College E-Safety Policy in newsletters, the college prospectus and on the college website.
- Information and guidance for parents on E-Safety will be made available to parents in a variety of formats including face to face meetings