POLICY TITLE: Student ICT Acceptable Use Policy

STATUS: Non-Statutory

DATE of REVIEW: September 2021

**Introduction**

The Latimer Arts College recognises that the use of Information and Communication Technology (ICT) is a strong learning tool.

As such, students are encouraged to use ICT to support their learning and progress. This procedure is designed to safeguard students in accordance with government guidance.

**E-Safety Awareness**

Through ICT lessons, our Personal Development Programme (PDP) and assemblies, students will be taught about how to keep themselves safe online and how to manage and assess risk.

Information for parents and carers will be provided through information evenings, in our newsletters or posted on the college's website

Staff will receive regular training as part of the college's professional development programme

**Use of College ICT Devices**

Computers, Laptops, tablets and other ICT facilities are provided for learning purposes only. Students should use the provided ICT facilities for college purposes only.

**Use of Personal Devices**

Some students may be given access to the college wireless network on their personal electronic devices. Such students must not share access codes or passwords with others. This network access is to support and aid learning within college, and is a privilege, not a right, and may be withdrawn at any time.

The College does not provide secure facilities for students to store their personal devices. Students must keep their devices in their bags at all times, unless permitted to remove them by a member of staff. We would recommend that, where possible, students also keep their bags with them.

Use of personal devices for learning is always at the discretion of staff. If a device is permitted to be used in a classroom, it should be switched off and returned to a student's bag before leaving the classroom.

By bringing a personal device into college, and using it connected to the college network, students agree not to attempt to circumvent the college network security and/or filtering policies, attempted exploits of the technology, interfere with another student's use of the resources, or use technology resources with the intent of causing harm to others. This includes downloading programmes to bypass security or accessing and setting up proxies/VPN's.

Students are expected to keep personal devices up to date with current security patches and suitable anti-virus software.

Students are not allowed to use personal devices outside of the classroom, unless they are being used during college visits, field trips, or outside activities, as permitted by a member of staff.

Any form of distribution of videos or pictures of other students and staff is strictly forbidden.

The College is not responsible for any loss of, damage to, or additional costs incurred by a personal device that is brought into College. The decision to bring a device into college rests with the student and their parent/carer(s).

Personal devices connected to the college network may be monitored to ensure this policy is being adhered to, and as part of the College's safeguarding duties.

**Acceptable Use of ICT Provision**

Access to ICT is provided without charge to all students of the College to enable the carrying out of recognised learning activities. By taking advantage of these resources, students are agreeing to the contents of this policy.

**Privacy**

Computer storage areas (files) are College property. The IT Services Team, Principal and designated staff may look at any file, email, or other communication at any time to ensure that the system is being used appropriately. Students should not expect that their work and e-mails are private.

**Security**

Passwords should contain a minimum of six characters, be a mixture of lowercase, uppercase, numbers and symbols, be kept secret, and must never be revealed to anyone.

Students may not use any other user's username or password in order to access a computer.

If a student becomes aware of another user's password, or that other students are using someone else's username and password, they should report this to a teacher or IT Services as soon as possible.

**Software**

Students should not attempt to install additional software not provided by the College, onto College computers or devices.

**Viruses**

The College will take all reasonable precautions to reduce the risk of viruses entering the system through the internet or by any other means. Anti-virus software is installed on servers and all workstations and is updated daily. Students should take sensible precautions to avoid viruses getting onto ICT equipment that they use.

**Faults**

If any equipment is found not to be working, students must report this to the IT Helpdesk and not attempt to rectify the problem themselves.

**Acceptable Use of the Internet**

All users must be aware that the internet is, by definition, an international network. Users of that network may not be trustworthy or reliable, and material found on the internet may not be appropriate for general viewing.

Access to inappropriate sites will be blocked either by the College or the College's Internet Service Provider and nobody should attempt to bypass this. Students identifying inappropriate sites should refer these to the ICT Services team to be blocked.

No user may access, or attempt to access, any site, whether blocked or otherwise, which is pornographic, obscene, racist or in any other way offensive. No user may install, copy, store or transmit any such material at any time.

Chat rooms, social networking sites, text messaging systems, ring-tones and gaming-type sites are not a suitable use of College resources, and may not be accessed by any user at any time.

**Social Networking Sites (e.g. Facebook)**

Staff are not permitted to be in contact with current College students via social networking sites and students should not attempt to become a 'friend' with any member of staff.

No material may be posted that would damage public trust and confidence in the college. Students must not post derogatory or inappropriate comments and/or images about other students, staff or about the College. "Light-hearted" comments will not always be interpreted as such by others and should be avoided. If in doubt – do not post.

Students using social networking sites should set the privacy levels on their accounts to maximum i.e. only people on their friends list should be able to view their pictures/private information etc. Care should be taken to avoid publishing personal information that could assist an attempt at identity theft.

Students should bear in mind that it is possible for another person to post a photo on their profile in which another user is named, so it is important to think about any photos that a user may appear in. On Facebook, it is possible to 'untag' a user from a photo. If a user does find inappropriate references and/or images of themselves posted by a 'friend' on-line they should contact them and the site to have the material removed.

Users should make sure that they regularly check and refresh their site page to ensure it is free of any inappropriate comments and/or images.

Inappropriate content can be reported to CEOP. The College's Designated Safeguarding Lead (DSL is CEOP trained.

**Acceptable Use of Email**

Our College e-mail system can be used for:

- Any activities which support the curriculum or college administration
- To enable students to submit homework
- To enable students to transfer college work between home and college

Our college e-mail system will not be used for:

- The distribution or forwarding of material which could be taken to be offensive by anyone reading the message
- Sending material which contains abusive or offensive language
- Sending messages which may be threatening or bullying in nature
- Emails that do not meet the requirements of the Data Protection Act or General Data Protection Regulations
- Any activities which involve personal financial transactions during college hours
- Forwarding chain letters
- Forwarding large graphics (pictures)
- Sending viruses/malware/ransomware/phishing scams or hoax messages
- Participating in non-educational social networking, newsgroups and chat rooms

**General Principles**

The College provides all students, subject to agreeing to this policy, with a College e-mail address. This should be used only for communications related to college work and not for personal use.

Students should have a personal e-mail account through their home Internet Service Provider (ISP) or a web based account for private communications.

The use of this account may be monitored by the College.

E-mail is a very powerful communication tool, however some points should be made regarding its safe and proper usage:

- When sending an e-mail, the subject line should accurately reflect the content of the message
- When sending e-mail students should ensure that they have carefully thought through what they are sending first.
- E-mail is the equivalent of a written document and can be used as an evidential record. With this in mind, care and consideration should always be taken before sending an e-mail.
- All unencrypted e-mail communication can be intercepted at any point between you and the recipient. Sensitive or confidential content should not be sent via e-mail, unless you are confident that appropriate safeguards, such as encryption, are in place and set up correctly.