Name of Policy:	**IT Acceptable Use Policy (AUP) for Students**
Last Approved:	June 2020
Approved By:	Leadership Team
LT Owner:	Jason Dear

Information Technology (IT) is a powerful and exciting resource which will support and enhance your learning. However, you must take responsibility for your use of IT and make sure that such usage is safe, responsible and legal. It is important that you know how to protect yourself from the risks associated with radicalisation, extremism, forms of abuse, grooming and bullying. If you feel unsafe, or if you are harassed or intimidated by anyone, you must report it to a member of staff. All concerns will be taken seriously.

Access to computers and other IT devices used by students whilst at College is a privilege not a right. This access requires students to be responsible – this includes access to IT provided by the college and personally owned devices. Some ways in which you can be responsible include:

- Not forwarding inappropriate messages**.** Stop cyberbullying by reporting it
- **Blocking** 'friends' who post negativity
- Never give any personal information out about yourself (or anyone else) over the internet
- Remembering that on the internet people can pretend to be who they are not
- If you use chat rooms, use a different chat name than your user name or email address
- Be wary of ANYONE who wants to know personal information about you.

No ICT device, whether College provided or personally owned, may be used for the bullying or harassment of others in any form. This AUP applies to IT Systems & devices supplied by the College and also to personal devices connected to the College wireless network.

Computer, IT & Internet Usage at Long Road Sixth Form College

1 A network account will be made available to you at the start of your courses and remains active whilst you are a student at Long Road Sixth Form College.

2 You must take care to protect your password and should not allow your account to be "shared" by other people

3 The College reserves the right to access any network account if it suspects the user of the account may be misusing the computer facilities or contravening this policy. IT Services reserves the right to quarantine any software or data that contravenes the IT Acceptable Use Policy. Before data or software is either moved back or deleted, a member of the Leadership Team (LT) shall approve this.

4 Students are advised that their network activity, including all online communications via the College network may be monitored. Logs of web browsing are kept for a minimum of six months. When unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to check and/or confiscate personal ICT such as mobile phones.

5 College email is provided to assist with your studies and to provide an effective communication between staff and students. Students may use their College email to contact people outside College. It is essential that your emails:

➢ Use appropriate language
➢ Do not contain defamatory or offensive material or material of an infringing or illegal nature
➢ Do not contain any financial data.

6 You should be aware that at the end of your course, your email will no longer be available.

7 You are provided with a College U: Drive where you should store all your work. You can, if you need to, use USB Sticks/Drives or your College provided OneDrive cloud files area. However you are advised to keep a copy of your work in the U: drive, as this is backed up in the event that your files are corrupted, lost or deleted.

The following are not permitted within the College environment (this extends beyond the College premises to include remote access to the College network):

- The use of any software and/or hardware to circumvent the College web filtering, security software or firewalls.
- The use of anonymisers (e.g. TOR Browser) or attempting to access anonymised networks.
- The use of Virtual Private Network (VPN) software, except where you have the appropriate authorisation from the IT Services Manager.
- Sending or displaying defamatory or offensive messages or pictures.
- Harassing, insulting or attacking others.
- Uploading, downloading, forwarding or using any material which is likely to be unsuitable for children, obscene, abusive, sexist, racist or defamatory. This applies to any material of a violent, dangerous or inappropriate context.
- Accessing information, visiting websites or engaging in any type of behaviour that could be seen as a significant breach of the College values, fundamental British values of democracy or the rule of law.
- Running software or installing any executable file on the College's equipment other than that provided by the College, except where you have written the software as part of your course of study or where you have the appropriate authorisation from the IT Services Manager.
- Connect any computing device to the College network other than a wireless device connected to the _LRSFC_WIFI wireless network without the express prior permission of the IT Services Manager.
- Using any portable applications running from removable media or College drives.
- Running or installing peer-to-peer downloading / uploading applications on the College network or computers.
- Damaging computers, computer systems or computer networks.
- Violating copyright laws – do not copy, store or use material which would infringe the copyright of another person, copyright applies to all text, pictures, video, sound, music and software.
- Using others' passwords or accounts.
- 'Hacking' into College systems, others' folders, work or files for any reason.
- Intentionally wasting limited resources (e.g. staff time, printer ink or paper), disrupting or corrupting the work of others, and other misuse of computers such as the introduction of 'viruses' / malware.
- Playing games other than as part of your course in a designated classroom with the teacher's permission. Games deemed to be of a violent, pornographic or gambling nature are not permitted anywhere in college.

.

Sanctions

Violations of the above rules will result in a temporary or permanent ban on internet / computer use. Additional disciplinary action will be added in line with existing Student Disciplinary Procedures.

- Your parents / carers will be informed.
- When applicable, Police or Local Authorities may be involved.
- If necessary, external agencies such as Social Networking or Email Member sites may be contacted and informed.

Additional Sources of Information and Guidance

- ➢ Cyberbullying: www.stopcyberbullying.org
- ➢ Child Exploitation and Online Protection: www.ceop.gov.uk
- ➢ Let's Talk About It (Preventing Violent Extremism): http://ltai.info