Moorlands Learning Trust

Student Acceptable User Policy

FAILURE TO COMPLY WITH THESE REGULATIONS MAY RESULT IN SANCTIONS OUTLINED IN THE SCHOOL'S E-Safety and RELATIONSHIPS POLICIES.

1. ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS

Name of Student

When using the school's ICT systems, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, racist, derogatory, criminal or pornographic in nature (or create, share, link to or send such material)
- Use the school systems in any way which could harm the school's reputation
- Access social networking sites or chat rooms unless specifically asked to by a member of staff for learning/research purposes
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network, including USB memory sticks
- Share my password with others or log in to the school's network using someone else's details
- Take or manipulate photographs of other members of the school community including staff without checking first
- Access, modify or share data I am not authorised to access, modify or share; or attempt to access or modify systems or devices settings without authorisation including adding a VPN (Virtual Proxy Network)
- Use the school systems to upset, harass or bully others

- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems
- I will take all reasonable steps to ensure that devices are secure and password-protected when using them outside school.
- I will secure my workstation if leaving it unattended
- I will let a member of the pastoral/safeguarding team know if any material has upset, distressed or harmed me or others.
- I will always use the school's ICT systems and internet responsibly
- I will make use of school ICT systems and avoid printing unnecessary material

If you are using your own device to access school emails and other data you will confirm the following:

• software security will be kept up to date for anti-virus/operating system patches etc

• the device will be password protected/encrypted or secured with biometric access

• ensure that any school data is securely deleted before selling/disposal of a device

• that under no circumstances will any form of 'jailbroken' or 'rooted' device be used to conduct school work or business.

Signed (Student)	**Date:**

Reviewed June 26
Approved June 26
Review Period 1 year