Student Acceptable Use Agreement
Online Safety Rules

Students are expected to read this agreement with their parent/carer and to sign and follow the terms. Parents are requested to sign below to show their awareness of student expectations in online safety. Any concerns can be discussed with their class teacher or the Head of Online Safety, Ms. Asaria.

- I will only use the school ICT systems, including the internet, email, VLE, tablets, digital video, mobile technologies etc. for purposes agreed by the school.
- I will not download or install software on school computers or laptops.
- I will only log on to the school network/ VLE with my own user name and password.
- I will keep my password secure and change it regularly.
- I will only only communicate with staff online via my school email address and the VLE, and will NOT search or add staff as friends or contacts on any other social network site.
- I will make sure that all online communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet, social media and related technologies at school and outside of school. This includes communicating with trusted people I know (not someone I have met online) and ensuring my security settings are set to private
- I know that the minimum age for using social network sites like Facebook,Instagram, Snapchat and Twitter is 13
- I will ensure that the resources I access are appropriate.
- I understand that cyberbullying is unacceptable, and will not use technology to bully, impersonate, harrass, threaten, make fun of or upset anyone, at school or outside.
- I will not browse, download, upload, post, retweet or forward material that could be considered offensive, harmful, extremist or illegal.   If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and my parent or guardian are aware.
- If I am worried about anything, I will report it immediately
- I must not take, store or forward photos or video footage of pupils or staff other than for school purposes in line with school policy, nor distribute it outside the school network or share on any social network site without the permission of the Headteacher.
- I will ensure that my online activity or use of mobile technology, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.
- I understand access to the school ICT Network and services will cease on my final day of school.

-- ✄ --

Student and Parent/Carer to complete, using CAPITAL letters:

Student Name: …………………………………………………..   **Tutor Group:** …………………….........
Understands and agrees to comply with the Student Acceptable User Policy and follow the Online Safety rules to support the safe and responsible use of ICT, at school and outside of school.

Student Signature: ………………………………………………

Parent/Carer Name: ……………………………………… **Parent/Carer Signature:** ……………………………………

Date: ……………………………

Greenford High School
Student Acceptable User Policy (AUP) – updated September 2018

Our Online Safety Policy has been written by the school, building on Ealing's model policy (with acknowledgement to Ealing Council, Hertfordshire Grid for Learning, LGfL, South West Grid for Learning, and Ofsted guidance)

The Aim
Our Online Safety Programme at Greenford High School is aimed at equipping young people with the knowledge and skills to identify, manage and reduce online risk, so that your child can get the most from the internet and technology, whilst staying safe.

Students: As a member of Greenford High School, students are entitled to access the school ICT Network. The Student AUP is aimed to ensure that you, as a student, can use the school network - Internet, Email, VLE and other technologies available such as mobile devices, both at the school and externally - in a safe and secure way, and that everyone is able to take advantage of the potential of ICT to support their learning in a responsible and safe manner. To do this students need to understand the rules and systems that are in place to protect them, to ensure that our school system is secure and that no one is subject to bullying, harassment or abuse.

Parents: Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in a safe and responsible way. Greenford High School will take every opportunity to help parents/carers understand online safety issues through online safety training and awareness raising at parents' evenings, and have access to useful information via parent leaflets, letters, website and information about national and local campaigns. Parents and carers have a responsibility to monitor their child's use of technology to support the *school* in promoting good online safety practice and to follow the guidelines outlined in this policy.

Policy
This policy forms the basis of an 'acceptable use' agreement form that students and parents/carers at Greenford High School are required to sign. This policy and Acceptable User Agreement extends to all hardware and software; both fixed and mobile internet technologies provided by the school (such as PCs, laptops, mobile devices, webcams/camera/video recording devices, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, or brought onto school premises (mobile phones and other mobile devices), whether accessed from the school or externally, irrespective of who owns the device and how the network is accessed. Breaches of the agreement usually result in a ban from the use of the ICT facilities including confiscation of devices, and in action being taken under the Greenford High School disciplinary procedure where necessary. Policy breaches may also lead to criminal or civil proceedings.

NB – Users of the network may be held liable for costs incurred for repair and/or replacement of equipment where the damage was caused by misuse.

Educational Purpose
The Greenford High School Network has been established for an educational purpose. The term "educational purpose" includes classroom 'learning' activities, purposeful communication, career development and quality research activities using the internet. Students may use the network for limited personal use, only before or after school hours and in strict adherence to the 'Unacceptable Uses' outlined below.

Student Internet, VLE, Email & Mobile Communications
Use of the Internet, Virtual Learning Environment (VLE), Email or other communication technologies at school and externally for purposes other than those outlined below will result in the suspension of Internet access and/or confiscation of devices for a fixed period of time.

1. Inappropriate Access to Material.
   a. You must not use the Greenford High School Network to access internet material that is inappropriate or offensive. Staff have the right to decide what they consider to be inappropriate and offensive.
   b. If you mistakenly access inappropriate information on the internet, you should immediately tell your teacher, or a member of staff. This may protect you against a claim that you have intentionally violated this Policy.
   c. You may not use the Greenford High School Network for commercial purposes. This means you may not offer, provide, or purchase products or services through the Greenford High School Network.
   d. You may not use the Greenford High School Network for political lobbying. But you may use the system to communicate with elected representatives and to express your opinion on political issues.

2. You may use web-based Email for school and personal use. The school reserves the right to block any email services that they consider to be unsafe or inappropriate. All emails sent and received are considered the responsibility of the user. You must not send emails which could cause offence to others. You must not access emails in school which contain material that could be considered inappropriate or offensive, therefore if you have any doubts about emails sent to you do not access them.

Misuse of Email, Mobile Technologies and the Internet
Use of email or messaging systems and the internet in lessons is at the discretion of the teacher in charge of the class.

Unacceptable Uses
The following uses of any ICT facilities within school and outside of school are considered unacceptable:
1. Personal Safety:
   a. You must not email or type into web pages or social media any personal contact information about yourself or other people. Personal contact information includes your telephone, school address and home address.
   b. You must immediately tell your teacher, staff member or a member of the ICT staff if you receive any message or access any image or text that you think is inappropriate or makes you feel uncomfortable.

2. Activities:
   a. You must not attempt to gain unauthorised access to the Greenford High School Network or go beyond your authorised access. This includes attempting to logon through another person's account or access another person's files.
   b. You must not make deliberate attempts to disrupt the computer systems, for example unplugging any cables or attempting to change any system settings.
   c. You must not access, delete or copy school data that you haven't been given permission to use.
   d. You must not intentionally introduce computer viruses to the school network system.
   e. You are responsible for avoiding plagiarism and must adhere to all copyright guidelines – this includes the download of any music, video and other materials which are copyrighted.
   f. You must not use any camera or video facilities on your mobile phone or any mobile device including your during the school day, whether at school or externally, unless this is part of a learning activity or authorised by a member of staff.
   g. Digital images or video footage of students and staff must not be posted to any website, social media platform or passed to any person outside school.
   h. You must not use the Greenford High School Internet access for any business purpose including buying or selling. This includes development of websites for other parties.
   i. You must not consume food or drink in the computer areas. These items should be left in your bag (for lunchtime clubs, this is at the discretion of the teacher)

3. System Security:
   a. Each student is responsible for keeping their login secure, taking all reasonable precautions to prevent others from being able to use it. **You must not let any other student know your password and change it immediately if you are in any doubt.**

b. Always log off or lock the keyboard (using **Ctrl + Alt + Delete**) when leaving a workstation, even for a short while.

c. No user should log on as someone else, nor use a computer which has been logged on by someone else.

d. You are not allowed to use a computer allocated to a member of staff.

e. You must immediately notify your teacher, ICT Support Staff or the Network Manager if you have identified a possible security problem. Do not go looking for security problems because this may be construed as an illegal attempt to gain access.

f. You must avoid the inadvertent spread of computer viruses. Email attachments that are suspect or from unknown sources should not be opened.

g. You must not attempt to download computer programs or games from the Internet

h. You must not try to load computer programs or games onto the Greenford High School Network or attempt to run programs that are not accessed through the normal menu structure, such as via any portable application device

4. Email, Social Media and Technology Misuse:

a. School Emails are automatically monitored and filtered. You must not email information that could cause damage, danger or cause disruption.

b. All electronic messages must be phrased using acceptable language and in an acceptable tone.

c. Never open an attachment or click on a link sent by someone you do not know or by someone you are concerned about.

d. Never reveal personal details about yourself to a stranger, such as address or telephone number, or arrange to meet someone online.

e. You must not use any ICT facilities (in or out of school) to bully another person. If you are told by a person to stop sending messages, you must stop.

f. You must not forward any electronic communication that was sent to you privately without permission of the person who sent you the message.

g. You must not email or electronically send/post/forward/tweet/share private or offensive information about another person.

h. You must not email or electronically circulate chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

i. If you are bringing personal USBs, cameras and mobile phones/devices to school, make sure that they are kept in a secure location at all times and be aware of personal photos and information already on these devices – consider locking devices and removing any personal content that should not be viewed.

5. Misuse of resources:

a. There are only a limited amount of computers available outside lesson times. Priority will always be given to users who need to use the computers for educational and careers purposes.

b. You must avoid unnecessary printing. Printers must only be used for school purposes. Students are not allowed to print personal pages and if found doing so will be expected to pay for the printouts and may receive a ban from the ICT facilities. A record of all printing is logged automatically by the Network.

c. Accessing and playing games via the Internet is not allowed. However a limited number of 'games' do have some significant educational value and these 'games' are the only ones you are permitted to access if directed by a member of staff.

d. You must not misuse or neglect any equipment in such a way so that it is likely to damage or destroy any school property.

e. You will not remove any ICT equipment from its position without the express permission from the Network Manager or a member of the ICT staff.

Other Technology - Personal Digital Assistants (PDA), memory cards, USB storage drives, tablets and anything else that can be used to store, transmit or manipulate data should be used responsibly and in accordance with Greenford High School's Acceptable Use Policy.

6. Monitoring of the network:

a. You should expect only limited privacy in the contents of your personal files on the Greenford High School Network. The school routinely monitors all files stored on the Network.

b. You should be aware that the ICT Staff routinely monitor the screens and usage of students.

Personal Responsibility

Students should be aware of the following:

a. Your actions on the Greenford High School Network are logged continuously. This includes the workstation/device you used, how long you were logged on for, what software was used and any printing you do.

b. All web pages accessed by a workstation/laptop on the Greenford High School Network are logged with the date and time of access.

c. Both these logs can be used to track specific actions by users or workstations at any given time.

d. Details and/or printouts of any unacceptable material or Internet access may be posted home to parents/carers/guardians and the students' access to the school network and tablet/laptop device suspended.

Discretionary Rights

Greenford High School reserves the right to vary the terms of this policy at any time and without prior notice. Students will be informed of any such changes. The school has the right to withdraw your access to the Network. The decision of Greenford High School is final.

Writing & Reviewing this Policy

o Staff, pupils and governors have been involved in creating/reviewing the Online Safety policy through consultation and meetings with our Online Safety Committee, Senior Leadership Team, the Child Protection Team, Head of Online Safety, Local Authority and the school's student CyberMentors.

o The policy and procedures are aligned with the Child Protection, Behaviour and Anti-Bullying Policies.

o There is an on-going opportunity for pupils and parents to discuss any issue of Online Safety that concerns them with Ms Asaria, the Head of Online Safety: Email: masaria@greenford.ealing.sch.uk or Tel: 020 8578 9152, Ext. 1602

o This policy will be reviewed annually and may be subject to change without notice. It will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

o The Acceptable User Policy and Agreement are distributed to new students as part of their induction and returned to our Admissions Officer, who logs/monitors them on the school's Information Management System.

o This policy has been read, amended and approved by the staff, Headteacher and governors on 3rd October 2018.

Please complete the Acceptable User Agreement and return to the school.