# Harlington Upper School ICT Acceptable Use Policy - Student

The school has provided ICT facilities for your use, offering access to a vast amount of information for use in studies and offering great potential to support your learning.
The ICT facilities are provided and maintained for the benefit of the entire school community, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all.
You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor.

**Equipment**

- Always get permission from the network manager before installing, attempting to install or storing programs of any type on the computers.
- All maintenance should be carried out by ICT support staff.
- Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Do not eat or drink in the vicinity of the ICT equipment
- Turn off any equipment when you have finished using it unless you are instructed otherwise by a member of staff

**Security and Privacy**

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- If you find a computer that another user has forgotten to log off from then inform a member of staff.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings is unacceptable behaviour.
- Your files and communications will be monitored to ensure that you are using the system responsibly.

**Internet**

See the Internet Acceptable Usage Policy

**Email**

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending of an email containing content likely to be unsuitable for children or schools is strictly forbidden.
- Spam
    - Be careful with your email address on the Internet.
    - You may receive spam if you publish your email address on a Web site, in a posting to a news group or in an online form (eg to send an electronic greeting card).
    - Never reply to a spam message, no matter how annoying! By replying, you let the sender know that your email address exists and then you are likely to receive more spam.
    - Never unsubscribe using links in spam email. This lets the sender know your email address is active – you are likely to receive even more spam
    - Never open attachments! Files attached to spam email often contain viruses. Delete the email immediately.

- The @harlington.org account provided by ICT support should be used for all communications with school staff and for communicating with other students for school work purposes.
- Webmail such as Hotmail should not be used at all in school.
- The use of email for bullying will be investigated and dealt with in accordance with the school bullying policy.

**Physical security**

- Main school students in an ICT room should be supervised by a member of school staff at all times. You should not be sent around the school to look for a vacant IT suite during lessons or to see if there are spare computers in an ICT suite when a lesson is taking place. You may be sent to an ICT room if a prior arrangement has been made with the teacher using that room by your teacher. The teacher in the ICT room will then be responsible for supervising you and you must follow their instructions. Alternatively, you may be sent to the library.
- In order to maximise access for Sixth Form Students, you will be allowed access to a vacant IT suite during lesson time. However to gain this access you will have to find a key holder. The last sixth former to leave the room must then find a key holder to ensure that the room is locked immediately. There must be at least two sixth formers in a room at any time.
- Outside of lesson times (this includes "Before School", "Break Times", "Lunch Time" and "After School") no student should have any access without direct supervision from a member of staff (i.e. the supervisor is in the room all the time that students are there).
- Doors to ICT rooms should be kept locked at all times when vacant. Inform a member of staff if you know that an ICT room has been left open.

**Images of students**

- Staff should only record images of students using school equipment, whether in school, or on a trip.
    - The use of personal digital cameras or camera phones by staff to record images of students is inappropriate.
- You should always ask another student or a member of staff for permission before recording their image. If they do not give you permission then you must respect their decision.
- Consider using group photos rather than photos of individual students.
- Any images of you held by the school will be deleted once their period of use has expired, or you have left the school.

**Personal equipment**

- Personal mobile phones and other portable devices such as portable digital assistants (PDAs) and MP3 players should be used according to school rules.
    - Use of personal mobile digital equipment for bullying will be investigated and dealt with in accordance with the school bullying policy.
- Staff must not give out their personal mobile phone numbers to you.
- Staff may ask you for your mobile phone number during a school trip or other event. You do not have to give it if you do not wish to. If you do give your mobile phone number to a member of staff, the record of your number will be destroyed after the trip or event.

**Please read this document carefully. If you violate these provisions you will be subject to disciplinary action.** Where appropriate, the police may be involved.

# Harlington Upper School Internet Acceptable Usage Policy - Student

The purpose of this policy is to ensure that users of the Harlington Upper School (HUS) network understand the way in which the Internet is to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk. Users should read this policy alongside the ICT Acceptable Use Policy.

## Policy statement

HUS encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise HUS's information and computer systems nor have the potential to damage HUS's reputation.
**Please read this policy carefully as you will be deemed to be aware of its contents.**

## Use of Internet facilities

HUS expects all users to use the Internet responsibly and strictly according to the following conditions: For the purposes of this document, Internet usage means any connection to the Internet via Web browsing, external email or news groups.

**Users shall not:**
Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other members of the school community

**If inappropriate material is accessed accidentally, you should immediately report this to your teacher so that this can be taken into account in monitoring.**

Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following illegal material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK

**If you accidentally access illegal material, you should immediately tell a teacher. Do not touch the computer.**

**Users shall not:**

- Use the HUS facilities for running a private business
- Enter into any personal transaction that involves HUS or the Local Authority in any way
- Visit sites that might be defamatory or incur liability on the part of HUS or the Local Authority or adversely impact on the image of HUS
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of HUS, or to HUS itself
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information
    - personal information
    - databases and the information contained therein
    - computer/network access codes
    - business relationships
- Intentionally interfere with the normal operation of the Internet connection, including the spreading of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion such as playing network games) that substantially hinders others in their use of the Internet

- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate

**Monitoring**
HUS will monitor and audit the use of the Internet to see whether users are complying with the policy. Any potential misuse identified by HUS will be reported to the E-Safety Co-ordinator and/or other relevant person.