Greenhill School

ACCEPTABLE USE POLICY AND INTERNET PASSPORT

2021/22

Welcome to Greenhill School

To qualify for Network, Internet and Email access, both students and parents must read, sign and return the agreement, attached to the end of this Acceptable Use Policy.

The staff of Ysgol Greenhill School strongly believe in the educational value of such electronic services and recognises their potential to support the curriculum. Every effort will be made to provide quality experiences to students and teachers using this information service. Remember that access is a privilege, not a right and that access requires responsibility in that students are responsible for their behaviour and communications over and on the network.

The Computer Misuse Act was enacted in the wake of the high profile hack of a mailbox belonging to The Duke of Edinburgh by Robert Schifreen and Stephen Gold. When they gained access to the login details of 50,000 Prestel customers, they were unable to be properly prosecuted as no relevant legislation existed. Instead they were tried (and acquitted) of forgery. In 1990 the Computer Misuse Act was introduced to plug this legislative loophole and make it illegal to gain improper access to a computer.

If the Computer Misuse Act 1990 is breached then a student or member of staff is likely to have the matter referred to other authorities including the police. The Computer Misuse Act 1990 identifies three specific offences:

- Unauthorised access to computer material (that is, a program or data).
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
- Unauthorised modification of computer material

Please read this document carefully, listed on the following pages are the provisions of this agreement. If any student violates these provisions, access to the Network, Internet and/or email will be denied and the student will be subject to disciplinary action.

Terms & Conditions of this Agreement

1. **Personal Responsibility as a representative of the school**
   I will accept personal responsibility for reporting any damage or misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest inappropriate language, unethical or illegal requests, racism, pornography, sexism, any use which may be likely to cause offence or attempts to disrupt or hack into the school's network.

2. **Acceptable Use**
   The use of ICT must be in support of education and research in accordance with the educational goals and objectives of Greenhill School. Students are personally responsible for this provision at all times when using any ICT resource.
   Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening/obscene material or material protected by trade laws. Use for commercial activities by for-profit organisations or personal enterprise is not acceptable.

3. **Privileges**

The use of ICT within the school is a privilege, not a right and that access requires responsibility, and that inappropriate use can result in that privilege being withdrawn. Students will participate in a discussion with a member of ICT staff as to proper behaviour and use of the facilities. Greenhill School staff will rule upon inappropriate use and may deny, revoke or suspend usage.

4. Network Etiquette and Privacy

Students are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

- **Be Polite:** Never send or encourage others to send abusive messages.
- **Privacy:** Do not reveal any personal information to anyone, especially the home address or personal telephone number of yourself or any other students.
- **Use Appropriate Language:** Remember that you are a representative of the school on a global public system. You may be alone with your computer, but what you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.
- **Password:** Do not reveal your password to anyone, even your friends. If you think someone has obtained your password, contact the ICT technicians immediately.
- **User Areas:** Your user area is not guaranteed to be private and will be treated like school lockers. Teaching staff have the ability to access the work in your user area in order to carry out marking and submission of work in relation to coursework and exams. IT Technical staff constantly monitors the contents of student’s user areas to ensure that users are using the system responsibly, manage storage space and to ensure compliance with copyright regulations. The IT Technical staff reserves the right to delete any unauthorised files, without notice.
- **Disruptions:** Do not use the network in any way that would disrupt the use of services to others.

- **Electronic Mail:** Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities in accordance with the RIPA[2] policy.

5. **Services**

Greenhill School makes no warranties of any kind whether expressed or implied, for the network service it is providing. Greenhill School will not be responsible for any damages suffered whilst on this system. These damages include: loss of data, loss of data as a result of delays, non-deliveries, missed deliveries or service interruptions caused by the system, errors or omissions.

Use of any information obtained via the network or other information system is at the student's own risk. Greenhill School specifically denies any responsibility for the accuracy of information obtained via its internet service.

6. **Security**

Security on any computer system is a high priority because of the large number of users. If you identify a security problem, notify a member of ICT support staff at once. Never demonstrate the problem to another student. All use of the system must be under your own username and password. Remember to keep your password to yourself and do **NOT** share it with friends.

Anyone caught disclosing passwords may have their access denied and may be subject to disciplinary action. Any user identified as a security risk, this includes, but is not limited to, attempting to bypass network security, attempting to install or installing unauthorised/pirated software or trespassing in others' folders, work or files may be denied access to the system and be subject to disciplinary action.

7. **Vandalism**

Vandalism is defined as any malicious attempt to damage, harm or destroy any equipment, data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the wilful damage of computer hardware, attempting to bypass network security and/or internet filtering, attempting to install or installing unauthorised/pirated software or the deletion/moving of data from its place of storage.

8. **Online Ordering Systems**

   One of the many facilities available via the internet is the ability to order goods and services whilst online. This technology is still undergoing development and several questions have been raised with regards to the issues such as security of online credit card ordering.

   Because of the security and other ethical issues attached to this facility, Greenhill School has a moral responsibility in this area. It is therefore strictly forbidden for students to use the internet for ordering goods or services regardless of their nature.

9. **Electronic Mail**

   Electronic mail (email) is provided by the LEA. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, inappropriate language, unethical or illegal requests, racism, pornography, sexism or any use which may be likely to cause offence.

   Disciplinary action will be taken in all cases.

10. **Chat Services**

    Students are not permitted to use chat services available on the internet.

11. **Internet Search Engines**

    Students are required to use internet search engines responsibly. If students are found to be searching for material unsuitable and in breach of this policy they will face disciplinary action. Students are strictly forbidden from attempting to circumvent or remove safety filters in order to access unsuitable or inappropriate material

12. **Electronic Data Storage & Backup**

    Greenhill school provide students with a user area (H:\) in which they can store their files for use with their work. It is the responsibility of the students to perform regular housekeeping on their user areas by deleting old or unwanted files.

Greenhill School follows a backup regime in order to support the recovery of the IT system in the event of a catastrophic failure, NOT to provide a backup service for pupils' files. In exceptional circumstances files will be recovered for pupils in accordance with the workload of the ICT support department.

13. Executable, Music & Video Files

Students are strictly forbidden from introducing executable files (e.g. '.exe, .com, .bat, .bin') to the network as these can sometimes contain harmful viruses. This includes, but is not limited to the copying of such files on to your user area (H:\) or attempting to run such files from USB memory sticks or flash drives.

Students are strictly forbidden from downloading executable, music and video files when using the school's internet provision.

14. **Bring your own device (BYOD)**

Subject to curriculum requirements, Students may be given the option of bringing in an Internet connected device to support their studies within school. After filling out the WiFi request form on our website (which also has fields needing to be filled out by parents/guardians) the student may bring in their device. The same level of filtering applies to these devices as is applied to school networked devices. Furthermore, students using BYOD must adhere to the Terms and Conditions laid out above. Failure to do so may result in the device being removed from the network and their Internet access revoked indefinitely.

Please now go back to the website and click on the link to fill out the form to let us know if you wish your son/daughter to be permitted to have Internet access at Greenhill.