Warwick Academy

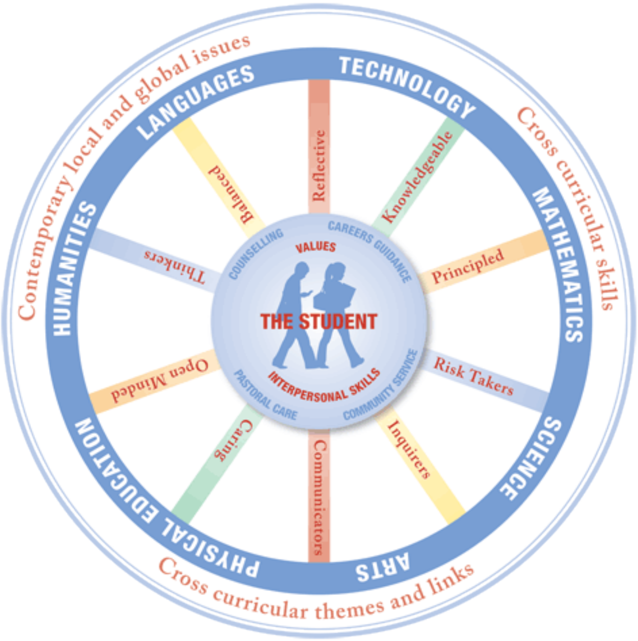
'so much more than a place to learn'

Internet User Policy

MISSION STATEMENT

Building on centuries of excellence, we provide an international educational environment designed for our diverse student body. Our innovative curriculum is delivered with a commitment to personalised pastoral care and enhanced by a dynamic co-curricular programme. We strive to create a culture of collaboration so that our students can become lifelong learners, global thinkers and successful leaders.

CURRICULUM MODEL



NOTES

Dated: June 2023
To be reviewed: June 2026
Staff involved: Strategic Team, SMT, PMT, IT Co-ordinator, Network Manager

Internet access is available to students and teachers at Warwick Academy. The Internet offers vast, diverse, and unique resources to both students and teachers. Our goal in providing this service to teachers and students is to promote educational excellence by facilitating resource sharing, innovation, and communication.

Students and teachers have access to:

1. E-mail in the form of Office 365 (not personal webmail alternatives).
2. Microsoft Office Suite for school use.
3. Access to the Internet.
4. The school Virtual Learning Environments (FROG and Firefly).
5. The cloud-based Microsoft OneDrive for document/file storage.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Warwick Academy has taken precautions to restrict access to controversial materials through a network filter. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. Warwick Academy firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the school.

Terms and Conditions of Use

1. **Acceptable Use** - The use of a school network account must be in support of education and research and consistent with the educational objectives of Warwick Academy. There is no limit on use for education and career development activities.

2. **Privileges** - The use of the internet and network is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges and other disciplinary action as deemed appropriate by the IT Co-ordinator, Network Manager, and PMT/SMT. Should the Network Manager, IT Co-ordinator, or any staff member identify inappropriate use or content they will consult with the appropriate person on PMT/SMT on what action to take. The Network Manager may suspend an account at any time as required.

3. **Access to the Internet** from any device attached to the school's network is only permitted through the school's network, where firewall protection, educational filtering, and dynamic monitoring is in place. The use of VPN's (Virtual Private Networks) is strictly prohibited as it bypasses network policies in place to safeguard students. The Internet is to be regarded as an educational tool and its use should therefore reflect such. The uploading and downloading of files to and from the Internet is permitted only in instances relating to acceptable educational instruction and/or research.

4. **Inappropriate use may consist of, but is not limited to:**
    a. Downloading of music, gaming, video, and executable files unless they are specifically needed for educational related matters.
    b. Use of file sharing networks.
    c. Use of social media, chat programs, and gambling.
    d. Accessing, or attempting to access sexually explicit and/or inappropriate content, material containing profanity or material advocating violence or discrimination towards others. If students inadvertently access such material, they should inform the Network Manager (or Teacher). This will protect them against the claim that you intentionally violated this policy.
    e. Illegal activities include spoofing, phishing, and activities that violate the copyright and intellectual property rights of others.
    f. Any form of cyberbullying (social networking sites, websites, e-mail, Teams chat, etc.). **NOTE**: Cyberbullying will be investigated if any distress is caused to other students/staff both in school and out of school.
    g. The Strategic Team reserves the right to modify what is deemed acceptable at any time.

5. **Network Etiquette** - Students are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:
    a. Be polite. Do not be abusive in your messages to others.
    b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
    c. Illegal activities (spam, phishing, etc.) are strictly forbidden.
    d. Do not reveal your personal information or the information of others.
    e. Do not share your network password.
    f. Note that e-mail is not guaranteed to be private. People who operate the system do have access to all school e-mail. Messages relating to or in support of illegal activities may be reported to the authorities.
    g. Do not use the network in such a way that you would disrupt the use of the network by other users.
    h. All communications and information accessible via the school network should be assumed to be school property.

6. **Security** - Security on the school network is a high priority, especially when the system involves many users. If students identify a security problem on the school network or via the internet, they must notify a Network Manager or Teacher. They should not demonstrate the problem to other users. Attempts to log on to the network as a Network Manager or as another user will result in cancellation of user privileges and/or other disciplinary action deemed necessary by the IT Co-ordinator, Network Manager, or PMT/SMT. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

    Classroom monitoring software will be installed on school computers and student laptops that use the schools’ network to monitor usage. This software only functions at school and not at home.

All users are responsible for any activity under their usernames/passwords and should take all necessary steps to protect their usernames/passwords. This should select an appropriate password, regularly changing their password, and ensuring that their workstation or laptop is locked when it is unattended.

Any equipment connected to the network must be sanctioned by the Network Manager. Access to network and internet resources must be done through the school infrastructure. The use of laptops must be in line with the schools' **Mobile Device Policy.**

7. **Vandalism** - Vandalism will result in cancellation of network access. Vandalism is defined as any malicious attempt to harm or destroy data of another user, internet, or any of the above listed agencies or other networks that are connected to any of the Internet backbones. This includes, but is not limited to, the uploading or creation of computer viruses. Any damage resulting from vandalism will involve the culprit being responsible for the cost of replacement and/or repair.

8. **Search and Seizure** – Only limited privacy related to the contents of your personal files while using the Warwick Academy network system can be expected. Routine maintenance of the network may lead to the discovery that this policy has been violated. An individual search will be conducted if there is reasonable suspicion that you have violated this policy or the law. The investigation will be reasonable and related to the suspected violation. The use of portable mass storage devices, such as USB pen drives, is permitted solely for the transfer of school related files from home to school and vice versa. They are however not recommended as online OneDrive access is safer. The IT Co-ordinator and Network Manager reserves the right to view the contents of such devices if it is believed that they contain files that violate this policy or that are a security risk to the network.

Students must understand and abide by this Internet User Policy. Any violation of the regulations above is against school policy may be unethical and may constitute a criminal offence. Violations will affect access, privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.