Acceptable Use Policy (AUP) for Computer and Internet Usage

An Acceptable Use Policy (AUP) is a document which addresses all rights, privileges, responsibilities and sanctions associated with the Internet and computer use. The school aims to maximise learning opportunities while reducing associated risks and will endeavour to advise students on good practice and safe usage of the Internet. NB: This policy must be read in conjunction with the school's Code of Behaviour (see the student journal or the school website www.dgs.ie).

Computing Facilities

Students are encouraged to make use of the school's computing facilities for educational purposes and are expected to act responsibly and to show consideration for others.

Use of Technology

Technology that can be used to store, transmit or manipulate data, such as SMART phones, MP3 players, Tablets, Personal Digital Assistants (PDAs) and USB media, must be used responsibly and, in accordance with the Acceptable Use Policy (AUP), even when not used with school equipment or network.

Conventional norms of behaviour apply to computer based information technology just as they would apply to more traditional media.

Rationale

The school supports and respects each family's right to decide whether or not to allow access to the Internet through the school network.

School computers and Internet connection should be used to enhance learning. Internet use and access is considered a school resource and privilege. If the school's AUP is not adhered to this privilege will be withdrawn and appropriate sanctions may be imposed. The AUP must be signed by students and their parents or guardians and returned to the school before access is granted.

Usage of the Internet therefore requires responsibility on the part of the user and the school's staff. These responsibilities are outlined in the school's Acceptable Use Policy.

As part of the school's educational programme students may also be offered WiFi access to the Internet which is monitored via the Department of Education and Skills (DES) Content Filtering Service (currently, Level 4).

The Internet is a global computer network which is not controlled by any organisation. This means that information may change, disappear, and be controversial or potentially harmful. Although the school actively seeks to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access objectionable material.

Students and their parents/guardians are advised that activity on the Internet is monitored and that these records may be used in investigations, court proceedings or for other legal reasons.

Privately Owned Computers and Devices

After accepting this AUP, and where permission is granted by school management, students may be able to access the secure school wireless network through a login and password provided by the school.

Privately owned devices (Tablets, Laptops, etc.), may only be used with the wireless network. Under no circumstances may devices be physically plugged into the school network connection points.

Insurance

The school cannot take any responsibility for the safe working, repair or security of personal devices whilst on, or in transit to and from, the school campus.

It is each student's responsibility to ensure that any electronic devices brought on to the school campus are suitably insured. The School's insurance DOES NOT cover these items. Insurance is the responsibility of parents/guardians and students.

It is strongly recommended that insurance cover is acquired for any devices used on the school campus. The school may be able to direct parents/guardians to appropriate insurance. See for example: http://www.gadget-insurance.ie

USER RESPONSIBILITIES

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

1. Students will be made aware of issues relating to Internet safety and the fact that the school will regularly monitor students' Internet usage.
2. Internet sessions will always be filtered through the DES Content Filtering Service (Level 4). In class situations the member of staff supervising Internet sessions will endeavour to ensure compliance with this policy.
3. Students will be informed what is acceptable and what is not acceptable in order to minimise the risk of exposure to inappropriate material.
4. Uploading and downloading of non-approved software will not be permitted on devices.
5. CD ROMs, DVDs and USB drives cannot be used without permission on school devices/hardware.
6. No electronic storage media or device may be connected to the school network without permission from the ICT Department.
7. Students must treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
8. Students must not visit Internet sites that contain inappropriate materials (e.g.: obscene, illegal, hateful or otherwise objectionable materials).
9. Students must report to a teacher any material of the above nature that they encounter.
10. Students must not disclose or publicise personal information about themselves or others.
11. Students must be aware that any usage, including distribution or receiving of information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
12. Students must not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
13. When using the Internet, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws, and all network users are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.
14. Mobile phone voice and text, SMS messaging or device instant messaging use by students during class time is not permitted.

EMAIL USAGE

1. Use of email may be subject to monitoring for security and/or network management reasons.
2. Students may not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
3. Students must immediately tell a teacher if they receive offensive email.
4. The forwarding of chain letters is banned.
5. Students should note that sending and receiving email during class time is subject to permission from their teacher.
6. If representing the school any email to an external party should be written carefully and authorised before sending by a member of staff.
7. Students must not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
8. Students must never arrange a face-to-face meeting with someone they only know through emails or the Internet.

PARENTAL RESPONSIBILITIES

1. Parents are requested to inspect the mobile device each evening to ensure that it is in good working order.
2. Parents should report, immediately, any damage, interference or issues relating to ownership, possession or use of the mobile device to school management.
3. Parents should inspect the mobile device and the installed Apps on a regular basis to ensure that there is no inappropriate material.

STUDENT RESPONSIBILITIES

1. Arrive to school each day with a fully charged mobile device. The School is under no obligation to supply a charging facility.
2. Keep the mobile device within a protective case and in a locked locker when not in use.
3. Do not let anyone use the mobile device other than your parents, teacher or other school-appointed person.
4. Report any problems, damage or theft immediately to your Form Teacher or Year Head.
5. Report any issues and interference created by any other student because of mobile device possession, use or ownership.
6. Do not leave the school without reporting any damage or interference that may have occurred during the school day.
7. Do not create, transmit, retransmit or participate in the circulation of content on devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the ICT department, or the school.
8. Do not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/guardian consent for minors) being recorded and the permission of an appropriate staff member.
9. Do not use Social Networks, access, download, create, store or transmit material that is: indecent or obscene; could cause any annoyance, offence, hurt or anxiety to others; infringes copyright (e.g. torrents); is unlawful; brings the name of the school in to disrepute.
10. Do not make inappropriate, hurtful or insensitive remarks about another student.
11. Do not attempt to download, store or install software to school computers.
12. Do not use Dundalk Grammar School IT resources to inappropriately obtain, store and/or distribute copyrighted material including music files and movies.
13. Do not attempt to introduce a virus or malicious code to the network.
14. Do not attempt to bypass network or system security.
15. Do not attempt to gain access to an unauthorised area or system.
16. Do not connect any device to the network that has access to the Internet via an authorised connection (data point) provided by the school without permission from the ICT Department.
17. Do not physically damage or vandalise any computer equipment or furniture e.g. Chairs, headsets etc.
18. Do not engage in activities that waste technical support time and resources.

    <u>The following points should also be noted:</u>
19. Students are responsible for the protection of their own school computer accounts/devices and should not give their passwords to anybody. It is recommended that devices are password protected.
20. Students must ask permission before sending documents to print on school devices/hardware.
21. Students must immediately report any inappropriate material either received or accessed.
22. Students should not logon to or use any account other than their own and should logoff when leaving a workstation, even for just a short period of time.
23. When on trips/tours or involved in activities outside the school, students should follow the guidelines set out by the relevant centre in relation to the storage of mobile devices.

LONG-TERM CARE AND SUPPORT OF DEVICES

Students and their parents/guardians are solely responsible for the care, maintenance and security of their devices.

1. Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions.
2. Students are responsible for ensuring that the operating system and all software on their device are legally and appropriately licensed.
3. Students are responsible for securing and protecting their device in school, and while travelling to and from school. This includes protective/carry cases and exercising common sense when storing the device. The School is not required to provide designated storage locations. However all students are provided with lockable school lockers and these should be used to store all valuable equipment.
4. Students should clearly label their device for identification purposes. Labels should not be easily removable. It is recommended that a tablet device is setup with a "Lock Screen" wallpaper background on the device which shows the student contact details i.e. name and telephone number.
5. Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

TECHNICAL SUPPORT

The school is under no obligation to provide technical support for hardware or software. The school may choose to provide this service to students if there are sufficient resources available in the school.

SANCTIONS FOR BREACH OF AUP

1. Misuse of the computer privileges may result in disciplinary action, including written warning, withdrawal of access privileges and, in extreme cases, suspension or expulsion. It is school policy to report any illegal activities to the appropriate authorities.
2. This Acceptable Use Policy (AUP) governs the use of the school's computer facilities and wireless network by students. Parents/Guardians who object to all or part of this AUP should inform the Headmaster in writing and by returning the agreement page unsigned. Once signed, parents are deemed to have accepted the contents of the AUP as a condition of the use of the computer facilities by their charge.
3. Where the school has reasonable grounds to suspect that a device contains data which breaches the AUP, the school may confiscate the device for the purpose of confirming the existence of the material.
4. Internet postings which are deemed to constitute a breach of this policy may be required to be removed; failure to comply with such a request may in itself result in disciplinary action
5. Access to the school WiFi network will be withdrawn with immediate effect for failure to adhere to this Acceptable Use Policy, or any other applicable school policy or guideline.
6. Access to the school Wi-Fi network may be restricted or withdrawn at any time, without notice, to ensure that the integrity and security of the network and/or other users are not compromised.
7. The iMacs in the Library are a limited resource and are to be used for academic purposes only. Any non-academic use will lead to withdrawal of all computer privileges.
8. The school reserves the right to sanction students for any un-forseen misuse of IT.

<u>The following websites offer support and advice in the area of Internet Safety:</u>

1. Make IT Secure - http://makeitsecure.org
2. NCTE - http://www.ncte.ie/InternetSafety
3. Safe Internet - http://www.saferinternet.org
4. Webwise - http://www.webwise.ie/