ACCEPTABLE USE POLICY (AUP) FOR COMPUTER AND INTERNET USAGE

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

Computing Facilities/Internet Access via MOBILE DEVICES

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

Any 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 If the school's AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions may be imposed.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 agreement (appendix 1) 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 AUP.

As part of the school's educational programme students may also be offered WiFi access to the Internet which is monitored via the PDST 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.

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 PDST Content Filtering Service (currently 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 or any other devices 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 will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
8. Students should 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 whether deliberately or accidentally.
10. The school will keep a record of all students who are granted Internet access.
11. Students must not disclose or publicise personal information about themselves or others. *(Please note the schools Code of Behaviour).*
12. Students will 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.
13. Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
14. 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.
15. Mobile phone voice and text, SMS messaging or any device that uses instant messaging use by students during class time is not permitted.
16. The use of the microphone or recording function on any device is strictly prohibited except under the direction and permission of the teacher.
17. Students must reserve the main (first) home screen for school app folders.

INTELLECTUAL PROPERTY RIGHTS

Subject specific educational resources designed by DGS staff remain the property of the school teaching staff who authored them. Students will be allocated a license to use them for as long as they are taking that subject or up to Leaving Certificate level. It is strictly forbidden to share school developed educational resources with another person not associated with DGS or download them for any other use.

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 any other person/s.
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, it 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.

PRIVATELY OWNED COMPUTERS AND DEVICES

Students will be able to access the secure school wireless network through their normal school login and password, after accepting this AUP. (maximum of 2 devices only)

Please note that privately owned devices (Tablets, Laptops, etc.), should only be used with the wireless network and under no circumstances should these 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. Please refer to the following link for an example of obtaining insurance for the student device; e.g. http://www.gadget-insurance.ie or http://www.mobilecover.ie.

PARENTAL RESPONSIBILITIES

1. Parents are requested to inspect their 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 via the school office.
3. Parents should inspect the mobile device and the installed Apps on a regular basis to ensure that there is no inappropriate material.
4. Parents are responsible for providing mobile device insurance on an annual basis and MUST return any school issued device and accessories in the same condition as received**.**

PASSWORDS

Upon student and parent/guardian signature on the Acceptable Use Policy (appendix 1) students will receive a Wi-Fi password unique to them

Students must enable a password/PIN on their devices, with auto-lock set to 5 minutes. They must not share their password with other students, but parents must know the password.

This password must not be shared with anyone and only used for the student's individual device or electronic devices.

CLASS BASED USE OF MOBLIE DEVICES: STUDENT RESPONSIBILITIES

1. All day student devices used in a classroom context must arrive to school each day fully charged. The school is under no obligation to supply a charging facility. Day students must take their device home each day and it must not be left on campus.
2. Designated boarding students will have access to charging facilities but must ensure that their devices are fully charged before timetabled classes. Boarding students will not be permitted to charge their device during the school day. Boarding students must ensure that when their devices are kept in their lockers when not in use.
3. Where a device is a replacement for paper textbooks, students should note that writing materials are still a requirement. Students must have the necessary writing materials (pen / paper).
4. Students must ensure the device brought to school has minimum 5GB memory space available to attend to the required learning tasks in the class.
5. Devices are to be kept within a suitable protective case (the school may make recommendation in this regard) and are securely locked in a locker when not in use, for example at break, lunchtime or school related activities.

6. Students must not allow anyone use the mobile device other than their parents, teacher or other school-appointed person.
7. Games, entertainment or social media may not to be seen or used during class time except under the direction of a teacher.
8. Report any problems, damage or theft immediately to your Form teacher or Year Head. Devices that are stolen must be reported immediately to school administration and the insurance provider.
9. Students must not go home from school without reporting any damage or interference that may have occurred during the school day. If you do so, school management will presume that the damage and/or interference took place outside of school time.
10. The use of 3G or 4G mobile WiFi on a device is not allowed. Only the school network is to be used by students while at school. Access to the school network must only be with the students own login and username details.
11. All work must be backed up and secured.
12. Mobile devices are to be left at home or in a secure place (e.g. locker) when students are on tours, trips and activities.
13. Students must ensure that mobile devices are not connected to any school-owned equipment without the permission of the school Headmaster, Deputy Principal or an appropriate ICT staff member.
14. Students must not create, transmit, re-transmit or participate in the circulation of content on their 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. The school's internet or email accounts must not be used for financial or commercial gain.
15. Students must not take photos or make video or audio recordings of any individual or group without the express permission of each individual (including parent/guardian consent for minors) being recorded and the permission of an appropriate staff member.

LONG-TERM CARE AND SUPPORT OF DEVICES

1. Students and their parents/guardians are solely responsible for the care, maintenance and security of their devices.
2. 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. ***Do not jailbreak the device i.e.*** *modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorised software.*
3. Students are responsible for ensuring that the operating system and all software on their device are legally and appropriately licensed.
4. 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.
5. Students should clearly label their device for identification purposes. Labels should not be easily removable. Device identification *Lock Screen* must show school, owner and contact details.
6. Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

LOST, DAMAGED OR STOLEN DEVICE.

If you lose or damage your device you must inform the ICT Co-ordinator /Year Head / Deputy Principal / Headmaster immediately so that your device may be tracked through iCloud, where possible.

The school is not responsible for loss, the financial loss, damage or otherwise to your device or loss of data / content.

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.

Teachers may from time to time recommend various applications that students may require in order to partake fully in a subject specific lesson. For example: 'iTunesU' - a free app or 'Explain Everything' approximately €4.99 to support revision for learning.

SANCTIONS FOR BREACH OF ACCEPTABLE USE POLICY (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 if warranted under the school's Code of Behaviour. 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 child.
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. Access to the school Wi-Fi network will be withdrawn with immediate effect for failure to adhere to this AUP, or any other applicable school policy or guideline.
5. 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 is not compromised.
6. All material on devices must adhere to the Dundalk Grammar School AUP. The access, sending, uploading, downloading or distribution of offensive, threatening, pornographic, obscene, or sexually explicit materials is strictly prohibited and will result in disciplinary action. (DGS Code of Behaviour/ Anti-Bullying Policy).
7. Dundalk Grammar School reserves the right to refer to external agencies in the event of illegal activity.

EXAMPLES OF POSSIBLE ACTIVITY / SANCTIONS (this list is not exhaustive)

Activity	***Sanction***
Possessing, viewing and / or distributing unacceptable material i.e. images, sound or video clips via email, USB, shared resources or other means e.g. YouTube / Vimeo /Social Media sites or Apps e.g. Snapchat, Instagram.	Note on VSWare for inappropriate conduct. After school detention or suspension up to and including expulsion Gardai informed where appropriate.
Installation or distribution of viruses / malware etc.	WiFi privilege removed indefinitely and Gardai informed.
Connecting to DGS wireless network by bypassing filtering / security measures (using software, proxy server websites etc.).	The automatic removal of WiFi privileges. Access to the school network will be removed indefinitely After school detention or suspension up to and including expulsion.
Taking of photos on personal ICT devices without expressed permissions.	The automatic removal of WiFi privileges. Access to the school network will be removed indefinitely After school detention or suspension up to and including expulsion.
Charging devices without permission.	An initial warning and note sent home. Repeated offence an after school detention and loss of WiFi privileges.
Accessing the Internet in class without teacher permission.	Note on VSWare for breach of ICT AUP. Friday after school detention.

The following websites offer support and advice in the area of Internet Safety:

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/