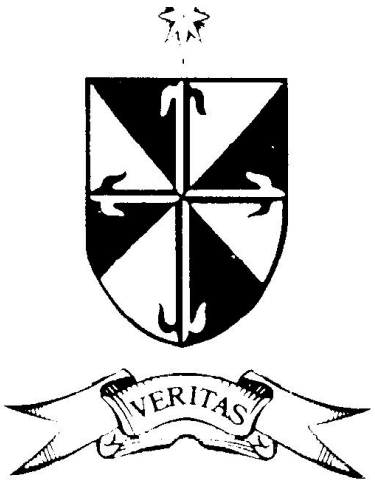
Dominican College Sion Hill



ACCEPTABLE INTERNET USE POLICY

AIM

The aim of Sion Hill's Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. We aim to create a culture of responsibility and wish to stress our partnership between family, school and student. Internet use and access is considered a school resource and privilege. If the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions, as outlined below will be imposed.

Sion Hill is committed to developing a first class eLearning environment as we recognise the benefits of eLearning in education which include:

- Access to world-wide educational resources;
- Opportunities to involve students actively in their own learning;
- Educational and cultural exchanges between students worldwide;
- Access to experts in many fields for students and staff;
- Communication with support services, professional associations and colleagues;
- Staff professional development through access to national and international developments, educational materials and good curriculum practice.

Sion Hill Strategy

Internet access will be planned to enrich and extend learning activities. Access level will be reviewed to reflect curriculum requirements and age of students. Sion Hill employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

- Internet sessions will always be supervised by a teacher;
- Filtering software and/ or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material;
- The school will regularly monitor students' Internet usage;
- Students and teachers will be educated in the area of Internet safety;
- Uploading and downloading of non-approved software will not be permitted;

- Virus protection software will be used and updated on a regular basis;

- The use of floppy disks, memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission. A virus check must always be done;

- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute;

- Students must respect the rights of others, the integrity of the computer system and they must obey all relevant laws, regulations and contractual obligations.

World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

- Students will report accidental accessing of inappropriate materials in accordance with school procedures.

- Students will use the Internet for educational purposes only.

- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).

- Students will never disclose or publicise personal information.

- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.

- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security, and/ or network management reasons.

Email

- Students will use approved class email accounts under supervision by or permission from a teacher.

- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.

- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.

- Students will note that sending and receiving email attachments is subject to permission from their teacher.

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the school.

- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.

- Usernames will be used to avoid disclosure of identity.

- Face-to-face meetings with someone organised via Internet chat will be forbidden.

School Website

- Students will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website

- The website will be regularly checked to ensure that there is no content that compromises the safety of students of staff.

- Website using facilities such as guestbooks, noticeboards or weblogs will be checked frequently to ensure that they no contain personal details.

- The publication of student work will be co-ordinated by a teacher.

- Students work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without the express written permission.

- The school will endeavour to use only digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission. Video clips may be password protected.

- Personal student information including home address and contact details will be omitted from the school web pages.

- The school will ensure that the image files are appropriately named, will not use students names in image file names or ALT tags if published on the web.

- Students will continue to own the copyright on any work published.

Cloud Computing

Students may have access to their school files both inside and outside of school time. School rules and this AUP apply to this facility and any inappropriate behaviour will be subject to the sanctions set out below.

Personal Devices

Students may be permitted to use their own devices in class with permission, and under the direction, of the teacher. In any other circumstances, students using their own technology in school (such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera, still or moving) is a direct breach of the school's Acceptable Use Policy.

Virtual Learning Environments

Virtual Learning Environments (VLEs) are web-based interfaces that assist learning and teaching by providing and integrating online resources and tools. Sion Hill is committed to developing a VLE in order to assist students to enhance their learning across the curriculum and provide a wide range of interactive activities, course support materials and access to structures of learning in a safe and monitored online environment. School staff are responsible for the development, upgrading and updating of course contents.

Familiarity with a VLE facilitates the acquisition of transferable ICT skills that can be used in other curriculum areas in school, in continuing education or training and in employment. It also encourages students to engage in valuable collaborative learning experiences and receive online mentoring support from peers and teachers.

Access to the Sion Hill VLE is a privilege not a right. It is provided so that students can develop their competence in ICT skills and general research skills. Students must use the VLE in a responsible manner. They must always maintain politeness and use appropriate language. Students are not permitted to:

- Use the VLE in such a way that it disrupts the use of the VLE by other users;
- Download software or other files without permission;
- Compromise others privacy by publishing, sharing or distribution personal information about any user;
- Use another user's password or allow other users to use their password;
- Engage in any activity which may result in the loss of or damage to another student's work; retrieve, send, copy of display offensive information, images or language; or
- Upload or use malicious code in any form within the VLE.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the internet.

Sanctions

We expect all students to abide by this AUP. Misuse of the Internet, school website or any other school technological equipment may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Ratified by the Board of Management 2013

Signed: _____

Letter to parents

Dear X,

Re: Internet Permission Form

As part of the school's education programme we offer pupils supervised access to the Internet. This allows students access to a large array of online educational resources that we believe can greatly enhance student's learning experience.

However, access to and use of the Internet requires responsibility on the part of the user and the school. Those responsibilities are outlined in the school's Acceptable Use Policy (enclosed). It is important that this enclosed document is read carefully, signed by a parent or guardian and returned to the school.

Although the school takes active steps to promote safe use of the Internet, I recognise the possibility that students may accidentally or deliberately access inappropriate or objectionable material.

The school respects each family's right to decide whether or not to allow their children access to the Internet as defined by the school's Acceptable Use Policy.

Having read the terms of our school's Acceptable Use Policy, you may like to take a moment to consider how the Internet is used in your own home, and see if there is any way you could make it safer for your own family.

Yours sincerely

_____

Sheila Drum

Permission Form

Please review the attached school Internet Acceptable Use Policy, sign and return this permission form to the Principal.

Dominican College Sion Hill

Name of Student: _____

Year: _____

Student

I agree to follow the school's Acceptable Use Policy on the use of the Internet. I will use the Internet in a responsible way and obey all rules explained to me by the school.

Student's Signature: _____ Date: _____

Parent/ Guardian

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

I accept the above paragraph _____ I do not accept the above paragraph _____
(Please tick as appropriate)

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing student's work on the school website.

I accept the above paragraph _____ I do not accept the above paragraph _____
(Please tick as appropriate)

Signature: _____ Date: _____

Address: _____ Telephone: _____

_____

_____

Cyber Bullying Policy

"Cyber Bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by any individual or group, that is intended to harm others".

Sion Hill will not tolerate any form of Cyber bullying by or against any member of the school community and such action will be taken extremely seriously and will be dealt with in accordance with this policy.

Introduction

1. Social media provide a dynamic and rapidly evolving means of communication. Mobile phones, chat rooms, websites and social networks, such as Facebook, play a significant role in many young people's lives as they interact with their peers and search for a social identity.

2. Inappropriate use of social media may lead to what is commonly known as Cyber Bullying.

3. Cyber bullying, like any other form of bullying, is the abuse of one person or group of people by another person or group of people. It is an affront to human dignity and will be treated in accordance with the principles and procedures of this Cyber Bullying Policy, the school's Code of Behaviour, the Child Protection Policy, the Acceptable Internet Use Policy, the Health and Safety Statement and the Policies on Dignity in the Workplace, Harassment, Sexual Harassment and other relevant policies.

4. Due to the instant, public, open and potentially permanent nature of access to material posted on social media and its capacity to multiply exponentially, a single inappropriate and offensive posting may constitute Cyber Bullying.

5. The school has a duty of care toward its pupils and staff. A safe and respectful environment in school is necessary so that teaching and learning can take place.

6. The school, together with other relevant parties (parent and/ or guardians, social media providers, Gardai etc) has a responsibility (though not the sole one) for the promotion of the responsible use of social media and the prevention of their misuse, with special reference to Cyber Bullying.

7. This Cyber Bullying Policy applies even when a student engages in inappropriate use of social media, when not under the direct supervision of the school; when there is a clear connection with the school and/ or a demonstrable impact on its aims, work reputation and/ or personnel.

Definitions

Social Media Technologies are defined as information and communication technologies (ICT), such as the internet, digital media or the mobile phone (e.g. text messages, group messaging services, instant messaging, personal websites, online personal polling websites, social media networks etc).

Cyber Bullying means any usage of Social Media Technologies that seeks to undermine or humiliate a member, or members, of the school community. This includes circulating or publishing through ICT, material recorded without consent for the purpose of undermining, or causing damage to, the professional or personal reputation of another person, whether considered a "joke" or not.

Policy

Cyber Bullying will be deemed a serious breach of the school's Code of Behaviour and Anti Bullying Policies, as well as other relevant policies, and will attract serious sanctions, up to and including suspension and expulsion. Allegations of Cyber Bullying may also be reported to the Gardai or other outside agencies as appropriate.

Any misbehaviour, including inappropriate use of social media, impacting on the health and safety of any member of the school community, will be treated with the utmost seriousness by the Principal and the Board of Management.

Reporting Procedure and Investigation

1. Any student or staff member who believes s/he has, or is being, subjected to Cyber Bullying, as well as any person who has reason to believe a staff member is being subjected to (or has been subjected to Cyber-Bullying) shall immediately report the matter to the Principal, the Deputy Principal or Year Head.

2. The Principal/ Deputy Principal of Year Head shall investigate all reports of such conduct in line with agreed school procedures. Cyber Bullying will be subject to appropriate discipline and sanctions, to be decided by the Board of Management. The seriousness of the violation will determine the sanction to be applied. This may include suspension or expulsion.

3. All involved parties will be informed of the results of investigations into Cyber Bullying.

Consequences for false accusation

1. The consequences and appropriate remedial action for a student found to have falsely accused another member of the school community of an act of Cyber Bullying range from positive behavioural interventions up to and including suspension or expulsion.

2. The consequences and appropriate remedial action for a school employee found to have maliciously accused another eimployee of an act of Cyber Bullying is that s/he may be disciplined. Such discipline will be in accordance with relevant legislation and the schools Dignity at Work Policy.

3. In circumstances where an investigation of Cyber Bullying is not proven, but the Board is satisfied that a genuine and reasonable complaint is made, no action will be taken against the complainant.

Discipline and Consequences

1. Some acts of Cyber Bullying may be isolated incidents requiring the School Authorities to respond appropriately to the individual committing the acts. Other acts may be so serious, or part of a larger pattern of Cyber Bullying, that they will require a response from outside agencies such as the Gardai.

2. Sanctions will be decided by the Board of Management and the seriousness of the violation will determine the sanction to be applied. This may range from positive behavioural interventions, up to and including suspension or expulsion. It should be further noted that Cyber Bullying using school technologies, is in violation of the school's Acceptable Internet Use Policy.

3. Intervention techniques to prevent Cyber Bullying and to support and protect victims may include appropriate strategies and activities, as determined from time to time by the Board of Management and Principal.

Appeals

Section 20 of the Education Act 1998 gives parents and students (aged 18 and over) the right to appeal certain decisions made by the Board of Management or by a person acting on behalf of the Board (expulsion; cumulative suspension of 20 days; refusal to enrol). In general, appeals must be made within 42 calender days from the date that the parents/ guardians were notified of the decision.

Reprisal or retaliation prohibited

The Board of Management will not tolerate reprisal or retaliation against any person who reports an act of Cyber Bullying. The consequences and appropriate remedial action for a person who engages in reprisal or retaliation shall be determined by the Board or Principal after consideration of the nature and circumstances of the act, in accordance with the principles of natural justice and Department of Education and Skills regulations and procedures.

The Board of Management and the Principal wish to encourage active reporting of all cases of Cyber Bullying and will support aggrieved persons throughout the process.

Ratified by the Board of Management in August 2013

_____