# AUP (Acceptable Usage Policy)
# St. Dominic's College, Cabra.

Date ratified by Board of Management:  9 November 2021
Last review date: 2012

## ACCEPTABLE INTERNET USAGE (AUP) & DIGITAL TECHNOLOGIES POLICY

**St Dominic's College, Cabra**, is committed to ensuring that all users including students, staff and parents / guardians will benefit from learning opportunities offered by the school's Information Technology (IT) system in a safe, effective and appropriate manner.
The policy is also mindful of the need to bring the key components of the school's mission statement - truth, freedom, justice, sincerity and joy - into the daily lives of all who attend or work in the school.

**The Aims of This Policy:**

- To promote the professional, ethical, lawful and productive use of St Dominic's College IT systems.
- To define and prohibit unacceptable use of the school's IT systems.
- To educate users about their IT Security responsibilities.
- To promote practices to ensure appropriate confidentiality and non-disclosure of the school's sensitive information.
- To describe where, when, why and how monitoring may take place.

**Policy Content**

1. Legislation & School Policy
2. Acceptable Internet Usage
3. E-Mail
4. Social Media Digital Citizenship
5. Personal Devices
6. School Website
7. Support & Further Information
8. Reporting on Inappropriate Content.
9. Misuse of Digital Technologies & Sanctions

### SECTION ONE - APPLIES TO STUDENTS

### 1. Legislation & School Policy that Govern and Guide Schools AUP:

- The Interception of Postal Packets and Telecommunications Messages Regulation Act, 1993:

This Act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence.

- The Video Recordings Act, 1989:

This Act prohibits the distribution of videos, which contain obscene or indecent material, which may lead to the depravation, or corruption of the viewer.

- The Child Trafficking and Pornography Act, 1998:

This Act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.

- The General Data Protection Regulations (GDPR) 2018:

These Regulations deal with the collection, processing and secure storage of personal data relating to individuals.

**School Policies that link to Acceptance Use Policy:**

- **Child Safe Guarding Statement (including Risk Assessment):**

Guided by the Children First Act 2015 & the Child Protection Procedures for Primary and Post-Primary Schools 2017.

- **Health & Safety Policy**

IT workstations have been ergonomically designed with care and are suited to student classwork, thus providing a comfortable working environment for all. Safety is of paramount importance within the IT lab and users of this room, must follow any teacher Health & Safety instruction at all times.

- **Homework Policy**

Teacher assessment is often completed through the use of digital technologies within reason where a student has access to a device and internet access if necessary.

- **Anti-Bullying Policy**

The schools anti-bulling policy incorporates acceptable use with regard to digital technologies and online behaviours.

- **Remote Teaching and Learning**

This Policy which was ratified in 2021 and outlines the responsibilities of students, teachers and parents with regard to the use of technology for remote teaching and learning.

- **Code of Behaviour:**

This outlines all school rules and sanctions in the event of breaches to school rules. Students are expected to follow the same rules for good behaviour and respectful conduct online as offline.

Misuse of school resources may result in disciplinary action. We have controls in place to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies.

Students are expected to alert their teacher immediately of any concerns for safety or security.

- **Misuse of the internet or of social media (Cyber Bullying)**

In accordance with the Anti-Bullying Procedures for Primary and Post-Primary Schools bullying is defined as follows:
Bullying is unwanted negative behaviour, verbal, psychological or physical conducted, by an individual or group against another person (or persons) and which is repeated over time.
The following types of bullying behaviour are included in the definition of bullying

- Deliberate exclusion, malicious gossip, and other forms of relational bullying,
- Cyberbullying,
- Identity-based bullying such as homophobic bullying, racist bullying, bullying based on a person's membership of the Traveller community and bullying of those with disabilities or special educational needs

- Cyberbullying is bullying carried out using information and communication technologies such as text, social networking sites, email, instant messaging (IM), apps, gaming sites, chatrooms, and other online technologies. Being the target of inappropriate or hurtful messages is the most generic form of online bullying. Cyberbullying uses technology to perpetrate bullying behaviour and does not require face-to-face contact. Cyberbullying is increasingly common and is continuously evolving.

- When using the internet pupils, parents and staff are always expected to treat others with respect. Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and should be dealt with, as appropriate, in accordance with the school's code of behaviour. However, in the context of this policy, placing a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour. Negative behaviour that does not meet this definition of bullying will be dealt with in accordance with the school's code of behaviour

- Reports of cyberbullying will be on a Bullying/Cyperbullying Incident Form and will be dealt with under the Anti-Bullying Policy and Code of Behaviour.

## 2. Acceptable Internet Use Policy:

**Internet Use:**

- Students are issued with a unique computer account username and password; this will grant them access to the school's ICT resources at a student's security level.
- Students must only use their own username at all times, unless instructed differently by a teacher.
- Students can only use the internet when supervised by a teacher.
- Students will use the Internet for educational purposes only.
- Online shopping is prohibited.
- Access to instant messaging services is forbidden.
- Blogging can only be used under teacher supervision.
- Students cannot use Online Gaming Apps, unless under teacher permission & supervision.
- Students cannot use school computer equipment for commercial gain except students in a school mandated Enterprise programme, e.g. TY Mini Company, LCA Enterprise.

**Inappropriate Content:**

- No user shall visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that relate to the promotion of: illegal acts, racist materials, pornography, child sexual abuse images, promotion of any kind of discrimination, threatening behaviour, including the promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school.

**E-Safety Education:**

- Students will be provided with information in the area of E-Safety Education: Students will be provided with information in the area of Internet safety.

**National Centre for Technology in Education:**

- St Dominic's College computer network is intended for educational purposes only. All activity over the network may be monitored and retained. Access to online content via the network is restricted in accordance with our policies and the Department of Education and Skills through its agency, the National Centre for Technology in Education.

**Web Filter:**

- Students are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material. If a site is blocked and a student believes it shouldn't be, the student can ask their teacher to submit a request to the site for review. This is done via the National Centre for Technology in Education's filtering service FortiGuard.

**Blocked Sites:**

- Access to social media sites like Facebook, Instagram and Twitter are currently blocked by the school WIFI. Social Media accounts may be set up by students with strict guidelines for its use for educational activities e.g. TY Mini Company. The teachers will monitor its usage in class time.

**Personal Storage Devices:**

- The use of personal USB memory keys, CD's or DVD's in school requires a computer teacher's permission and is not advised. Students should save school work to their school assigned google drive or the school network under their personal profile. Images / videos taken in class are uploaded to student's personal drive and wiped from the device. The school reserves the right to read all memory devices/disks and to check them for viruses.

**Software Installation**:

- Uploading and downloading of non-approved software will not be permitted.

**Downloading:**

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

**Virus protection:**

- Related software will be used and updated on a regular basis.

**Copyright:**

- Students must be aware of and comply with copyright issues relating to online learning especially in the areas of music or other media, and will refrain from distributing these in a manner that violates copyright licences.

**Copyright downloads:**

- Students cannot upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without necessary licensing permissions.

**Viruses:**

- Students must not create or propagate computer viruses or other harmful files.

**Networks:**

- Students must not carry out sustained or instantaneous high volume network traffic *(*downloading/uploading files) that causes network congestions and hinders others in their use of the internet.

**Plagiarism & Copyright Infringement:**

- Students will not copy information into assignments and fail to acknowledge the source. Students will not copy work from other students.

**School Security:**

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

**Digital Citizenship:**

- When using the internet, no one will undertake any actions that may bring the school into disrepute.

**3.Email.**

**Permission:** Students will use approved class email accounts with the permission and the supervision of a teacher. Students will note that sending and receiving Email attachments is subject to permission from their teacher.
**School:** Students should only use school email accounts for all school related communication.
**Respect:** Students will only use appropriate language, showing respect to teachers and peers at all times.
**Appropriate Content:** No one will send or receive any material that is illegal, obscene, and defamatory or that is intended to cause upset or intimidate another person.
**Reporting:** Students should report any aggressive or inappropriate behaviour directed at them or others.
**Account Privacy**: Students must not reveal their own or other people's personal details; such as addresses or telephone numbers or pictures when communicating via email.
**Face-to Face Meeting:** Accessing instant messaging chats is forbidden. Students will never use Email to arrange a face-to-face meeting with someone outside of school.

**4. Social Media & Digital Citizenship:**

- Students will only have access to sites, discussion forums or other electronic Communication forums that have been approved by the school.
- These forums will only be used for educational purposes and will always be supervised. Usernames will be used to avoid disclosure of identity.
- The school cannot control what Social Media Sites/Social Networking sites students access in their own personal time and for their own personal use, however students should be mindful to behave responsibly at all times as inappropriate online behaviours outside school can often affect the school community. In cases that are deemed necessary, disciplinary measures may be taken against a student in breach of our school policy.

**Digital Citizenship & Social Media:** Students should only use appropriate language and image on the internet or on any school virtual learning environment. Students should not post inappropriate personal information about their own (or any other person's) life, experiences or relationships. Students should ensure that anything they post online will not put them at risk.

Students should never publish full contact details, a schedule of their activities or inappropriate personal details in public spaces. Students should report any aggressive or inappropriate behaviour directed at them. Students should not share their passwords or account details with anyone else. Students should show respect to others and not use electronic mediums to upset, intimidate, harass or stalk other people.

**School Social Media Accounts:**
All official school social media accounts are used to promote the school within the wider community and facilitate parents, teachers and students with easy access to the most up to date information about school events and activities.
All Accounts will be monitored by a named teacher and the author of this account must liaise with this teacher on a regular basis.
Photographs, audio and visual clips will focus on achievements of students and activities in the school.

**School-Student Social Media Accounts & Acceptance Usage Policy:**
Student Leadership & Student Voice:
Members of our student council and various student leaders, may operate school twitter/Instagram sub-accounts.

- Students must seek permission from the principal before setting up this account.
- All Accounts will be monitored by a named teacher and the author of this account must liaise with this teacher on a regular basis.
- Photographs, audio and visual clips will focus on achievements of students and activities in the school.
- Content uploaded is for educational purposes only to promote student achievement.
- Students will not post material that is illegal, obscene, and defamatory or that is intended to cause upset or intimidate another person.
- Students will not post content that may breach copyright regulations or bring the school into disrepute.

**5. Student Personal Devices**
**Tablets/laptops & other Electronic Devices:** Students using their own technology in school should follow the rules set out in this policy. Students should only use personal hand held/external devices in school if they have permission. If there is a significant concern about inappropriate usage of a device during this lesson time, a student may be asked to submit their personal device to a teacher, who will in turn hold it and may if necessary hand it to Management to inspect the search history.

**Mobile Phones/Smartphones:** As Mobile phones are not allowed to be used within the school generally, they cannot be used within the classroom, unless granted permission by the teacher for Teaching & Learning Purposes of that specific lesson or part of that lesson. This does not include using Mobile phones for the purpose of listening to music. In this case students, must use the phone responsibly and for the intended purpose as outlined by the teacher. Students may be requested to turn their phones to flight mode to restrict any incoming personal messages while this lesson is being carried out. The phone must be switched off, when the teacher instructs and before the end of that scheduled lesson time.

Mobile phones cannot be used at any other time inside the school building, inside the first and last school bell of the day. The unauthorised capture of images, video or audio is in direct breach of the schools AUP. Connecting or attempting to connect to the school's network system (wired or wireless) is in direct breach of the schools AUP.

**6. School Website:**

- The purpose of the school website is to promote the school within the wider community. It will also facilitate ease of access for parents, students, staff and others to the most up to date information on recent events and activities in the school.
- Material intended for the web site will be gathered, read and approved by the relevant school personnel. An appointed member of staff will gather the materials for use on the school web site, which will then be updated regularly.
- Photographs, audio and visual clips will focus on achievements of students and activities in the school.
- Personal student information including, home address and contact details, will be omitted from the school web pages.
  - The permission of parents/guardians of students, staff members and any person whose name or photograph could be published on the website will first be sought before his/her name or photograph is published on the website.
  - Students, staff or others in the school community or associated with it, who publish work on the website will continue to own the copyright on their own work.

**VSware:**

- Logins and passwords for VSware should be kept personal and private. Parents / students should use VSware for the intended purpose.

***7*. Further Support Advice & Guidance on Internet Safety**

www.webwise.ie
www.education.ie
www.pdsttechnologyineducation.ie
NCTE (National Centre Technology in Education)
Wriggle

**Support structures:**

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

**8. Reporting on Inappropriate Online Activity:**

- Students should report all inappropriate activity to the supervising teacher in the room without delay and/or to the respective year head of the student's year group.

**9. Sanctions for Misuse of Digital Technologies and Internet Usage:**

1. Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases suspension or expulsion.

2. The school also reserves the right to report any illegal activities to the appropriate authorities.
3. Misconduct will be investigated and the Principal will make recommendations on any report of misconduct with regard to digital technologies and online activity. These recommendations will reflect on whether the incident is considered to be a mild or serious breach and may come with either a mild sanction or heavy penalty respectively.

## SECTION TWO – APPLIES TO STAFF

### 1. Staff Devices

**Insurance**

- School devices are school property and are therefore insured under the school insurance contents policy.

School devices are insured if damaged or stolen when on-site or off-site. This covers being out and about on school business, school tours or theft from a staff member's home.

If a device is being transported in a car it must be kept in the boot, out of sight at all times and the car must be locked.

- There is a €300.00 excess on any device in respect of which a claim is made.
- If your contract has ceased with the school, you have retired, are on Maternity Leave or Career break the Surface Pro must be returned to the Deputy Principal before you leave.

Authorised software is installed on your computer and you are not allowed to install anything on your own. Please talk to the IT Co-ordinator if you would like to download anything else.

- Data saved to local (usually C: and D:) drives will not be backed up, and will be lost if the computer breaks, gets stolen or is replaced, therefore it is highly recommended and it is your responsibility to store all your data on your personal One Drive account.
- The School may at any time and without prior notice audit the computers to ensure:

- Compliance with policy
- Staff take full responsibility for everything done on their portable computer.
- Staff are responsible for the care and safe storage of any computer equipment that has been issued to them.
- The term 'portable computer' covers any school-owned mobile computing device including: - Laptop or tablet PCs (Surface Pro and IPad)
- All school devices are encrypted to ensure an extra level of security.
- Teachers who use their own personal devices for school work are subject to the same guidelines of the AUP.

**Data Protection Responsibilities**

- You are personally responsible for ensuring the confidentiality of a student's personal data
- If Personal Data is saved to a USB drive ensure it is fully encrypted.
- If you process personal data (data that identifies a living individual) in the course of your work, you must do this in accordance with General Data Protection Regulation (GDPR) May 2018.
- Do not view sensitive information on the train, plane or in any public area. This provides an opportunity for onlookers.
- Do not allow family, friends or anybody else to use the computer which contains student information.
- When communicating information through email do no put names in the subject bar.
- Teachers who need to take images / record videos as part of a school activity should delete after uploading to the drive or to an external storage device.
- Do not disclose or share any sensitive information to other people if not under the expressed authorisation of the Principal.
- Do not leave printed documents around the printer as they may contain confidential data.

Signed:

Signed Frances Cooke
*Chairperson, Board of Management*

Signed Ann Comey
*Principal*

Date: November 9 2021

Date of Review: November 2024