**De La Salle College**

 **Macroom, Co.Cork**

 **Acceptable Internet Use Policy**

The aim of this Acceptable Use Policy (AUP) is to ensure that pupils will benefit from learning opportunities offered by the school’s Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions-as outlined in the AUP-will be imposed.

**School’s Strategy**

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

**General**

* Internet sessions will follow strict usage protocols.
* Filtering software systems 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 will be provided with training in the area of Internet Safety through their S.P.H.E programme.
* 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 personal memory sticks or Digital Storage Media in school requires a teacher’s permission.
* Students will treat others with respect at all times and will not undertake any action that will bring the school into disrepute.
* Students will never facilitate a third party to enter an online class. This is a major contravention of the school’s Code of Behaviour, with serious safety implications and potential consequences.
* Training on Digital literacy is provided through SPHE classes in Junior Cycle.
* The use of a fellow students profile without their knowledge will result in an immediate sanction.

**World Wide Web**

* Students will not visit (deliberately) 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 be familiar with copyright issues relating to online learning.
* Students will not copy or plagiarise into assignments.
* Students will never disclose or publicise personal information.
* 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.
* Downloading of materials or images not relevant to studies is in direct breech of the schools acceptable use policy.

**Email & Social Networking**

* Students will not send, like, share or comment on any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
* Students will not impersonate others/will not exclude others on social media.
* Students will not reveal their own or other people’s personal details, such as addresses, telephone numbers or pictures.
* Students will not arrange a face-to-face meeting with someone they only know online.
* Students will note that sending and receiving email attachments is subject to permission from their teacher.
* Students will not engage in behaviour that is in contradiction of the school anti-bullying policy.
* The school’s social media sites are carefully monitored by a number of staff. Any inappropriate comments/actions made in relation to the school sites will be copied, removed and the appropriate sanctions applied.
* Students will only contact their teachers through the use of Microsoft Office Teams between the hours of 09.00-16.00 unless an alternative time has been expressly agreed upon by their teacher.
* House exams will not be put up on Teams as any student who cannot attend a house exam will be given an estimated grade by their teacher.
* If a parent wishes to contact a teacher, they should ring the office and leave a contact number and email address which the teacher can use to contact them.
* It should also be kept in mind that the school may take a view upon any items published, by any means, if those items could bring the name of the school or any person working in the school into disrepute. This last consideration is not confined to term-time only.

**Personal Devices**

Students using their own technology in school should follow the rules set out in this agreement. Students will only use Personal hand-held devices (mobiles, USB etc) in class with teacher’s permission. When mobiles are used in class the mobile must be placed on the table facing up and must be put back in the lockers before the end of class. The use of handheld devices to take pictures is strictly prohibited in school.

**Legislation**

Information on the following legislation relating to use of the internet which teachers, students and parents should familiarise themselves with can be

obtained from the Government website [www.irlgov.ie](http://www.irlgov.ie)

* Child Trafficking and Pornography Act 1998.
* 1993 Interception Act.
* Video Recordings Act 1989.
* The Data Protection Act 1988.
* Data Protection Amendment Act 2003.

**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 as it becomes available.

* ***Advice to students.***
* (a) Respect other people. Remember that when you send a message to someone, you cannot see the impact that your words or images may have on the other person. That is why it is important to always show respect to people and be careful what you say online or what images you send. What you think is a joke may really hurt someone else. Always ask permission before you take a photo of someone. Please bear in mind that (except with the expressed permission of a teacher) the taking of, and/or subsequent dissemination of, still or video images is strictly prohibited in school. Breaches of this rule will be subject to sanction.
* (b) If you receive a rude or offensive message or picture about someone else, do not forward it. You could be assisting a bully and even be accused, yourself, of cyber-bullying. You might also be breaking the law.
* (c) Think first before you send. It is important to think before you send any images or text about yourself or someone else by email or mobile phone, or before you post information on a website
* Remember that what you send can be made public very quickly and could stay online forever. Parents, teachers, friends or future employers may be able to evaluate your character on the basis of your online footprint.
* (d) Protect your password. It is good practice to change your password on a regular basis and not to disclose it to other people. Choosing hard-to-guess passwords with symbols or numbers will help stop people hacking into your account and pretending to be you. It is also sensible to give your mobile phone number only to trusted friends.
* (e) Block the bully. Most responsible websites and services allow you to block or report someone who is behaving badly.
* (f) Don’t retaliate or reply. Replying to bullying messages, particularly in anger, may well be what the bully wants and can easily escalate matters very quickly.
* (g) Save the evidence. It is important to keep records of offending messages, pictures or online conversations. If you are intending to make a complaint, they will help you demonstrate what is happening and can be used by the school, Internet service provider, mobile phone Company, or even the Gardai to investigate the cyber-bullying.
* (h) Make sure you report incidents of cyber-bullying. You have the right not to be harassed and/or bullied online and you should report incidents of cyber-bullying which take place.
* The school draws a distinction between incidents which originate from within the school environs and those which occur outside. While the same standards apply at all times and in all places, it needs to be recognised that the school cannot be held responsible for students’ actions when not in the care of the school or its agents. The school will inform students about internet protocol and best practice in the area of internet usage, including the concept of "public domain". The school values parents’ support in reinforcing best practice in this area. Any cyber-bullying incident involving a student, as perpetrator or victim, is of concern, but especially when both perpetrator and victim are students, equally, social comment about a member of staff which falls under the categories listed above will not be tolerated.
* Any unauthorised photograph of any members of staff will be viewed in a serious light and will merit serious sanction.

**Sanctions**

Misuse of the Internet may result in disciplinary action, including withdrawal of personal devices, written warning, and withdrawal of access privileges, detention and in extreme cases, suspension or expulsion. The School also reserves the right to report any illegal activities to the appropriate authorities.

**Ratified Next Review**

25th Oct 2022 2023/2024

**Signed**

****

Chairperson of the board of management



Principal