ICT EQUIPMENT AND INTERNET ACCESS;

ACCEPTABLE USE POLICY

Acceptable Use Policy (AUP)

The aim of this AUP is to ensure that pupils will benefit from learning opportunities offered by Information Communication Technology (ICT) as well as Internet resources in a safe and effective manner. Internet and ICT equipment (including but not limited to; desktops, laptops, tablets, smart phones, smart watches, etc.) use and access is considered a 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 Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

The school recognises the benefits of ICT equipment and the wealth of resources available online for students' learning. Also this area is a huge part of students' lives and futures. As a school we aim to teach students how to interact with the Internet and computers in a safe and appropriate way. ICT equipment and Internet will be used to facilitate student learning and may also be used to reward positive behaviour.

It is envisaged that school and parent representatives will revise the AUP as needed. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

School's Strategy

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

General

- Parents are asked to monitor home use.
- Students, teachers, special needs assistants and parents will be provided with training and or links in the area of internet safety – PDST in school support, online training, peer support, parents evenings/online.
- A firewall is used on school devices to minimise the risk of exposure to inappropriate material and to block unsuitable sites. This is regularly updated.
- Uploading and downloading of non-approved software on school devices will not be permitted.
- Internet sessions will always be supervised by a staff member.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software must be used and updated on a regular basis.
- The use of personal floppy disks, memory sticks, CD-ROMs, or other digital storage media in school requires permission from a member of the ICT team.

Use of Information Communication Technology (ICT) Resources

St. Augustine’s ICT resources (e.g. email, computers, laptops, tablets, computer applications, networks, internet, intranet, facsimile, phone and other wireless communications devices, telephone, paging and voice mail systems and the like) are school property and are provided solely for school related activities.

Inappropriate use of school and personal devices; including hacking, pirating software, using school resources for non-school commercial activities, soliciting, distributing literature for outside entities, disclosing confidential information of the school, sending inappropriate e-mail or accessing inappropriate web sites (such as those advocating hate or violence, containing sexually explicit material promoting illegal activities), or using school resources in a way that violates the letter or spirit of the school’s policies or reflects negatively on the school is forbidden.

Users of the school’s information and technology resources must not share passwords. If you allow others to use your password or assigned resource, you will be held responsible for their use.

Consistent with national laws, the Board of Management reserves the right to monitor the use of its information and technology resources and to take appropriate disciplinary actions, or denying future access privileges in cases of misuse. Staff/student use of the school’s information and technology resources constitutes consent to such monitoring. All such monitoring will be conducted in accordance with law including, where applicable, the EU’s General Data Protection Regulation (GDPR).

World Wide Web (including Social Media)

- Students will only use the internet with the permission of a teacher, SNA or staff member.
- 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 never disclose or publicise personal information; examples are but not limited to: their own, staffs' or classmates' full names, Date of Births, addresses, email addresses, passwords, phone numbers, profile information or name and location of their school, etc.
- Students will not share other's personal information, photos or recordings or add others to social media groups without their consent.
- Parent(s)/guardian(s) and students are requested not to 'tag' photographs or any other content which would identify any children or staff in the school.
- Images or recordings of staff or students will not be taken or shared without consent.
- Pupils should not contact staff members via social media. If a staff member is contacted by a pupil, they should not engage with pupils and inform principal as soon as possible. Principal will contact parents to discuss such incidents.
- Students will not examine, change or use another person's files, accounts, usernames or passwords.
- 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.
- The school takes every reasonable precaution to provide for online safety, but it cannot be held responsible if students access unsuitable websites either deliberately or inadvertently.
- Students will treat others with respect, observe good "netiquette" (i.e., etiquette on the internet) at all times and will not undertake any actions that may bring the school into disrepute.
- It is important to note that the school's Anti-Bullying Policy should be read in conjunction with this policy. Parents/guardians and students should be aware that placing a once-off, offensive or hurtful internet 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.

Email

- Students may use approved school email accounts under supervision by, or with permission from, a teacher. Accounts will be deleted after use.
- 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, social media, chatpages or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Internet Chat-rooms, personal social media, personal blogs, etc. are not to be accessed at school.
- Usernames and secure passwords will be used to avoid disclosure of identity.

Distance Learning

- In circumstances where teaching cannot be conducted on the school premises, online platforms and tools, such as Zoom, Seesaw, Classdojo, Edmodo, Onedrive and school email will be used to assist with remote teaching, communication, sharing and messaging among staff, students and parents where necessary. These platforms/online tools need to be approved by the principal.
- Students are expected to uphold the same appropriate, safe and courteous conduct online as is expected offline.
- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication that have been approved by the school and sanctioned by the class teacher, for example (Zoom, Classdojo).
- Any electronic forms of communication will solely be used for educational purposes.
- When using these communication forums, parental permission for the child is implied, as the links for lessons are being communicated through parents. Essentially, by virtue of the children logging in to the resource, permission is assumed.
- It is the duty of the Parents to supervise children while using devices at home. Where possible students should be in a public room, seen by parents.
- Usernames and passwords will be provided to avoid disclosure of identity where possible.
- St. Augustine’s cannot accept responsibility for the security of such online platforms in the event they are hacked.
- Each staff member has been issued with a dedicated school email address which they can use to make contact with parents.
- Where it is necessary to contact a parent/guardian by mobile phone, staff members should change their settings on their phones so the recipient of the call sees “No caller ID”.
- For online platforms (Zoom, Classdojo, etc.) parents/guardians must consent to submitting their own email address for their child to access lessons on Zoom.
- Two staff should be present on any online sessions with class/students.

School Website

- Pupils may 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 pupils or staff. The publication of student work or images will be the responsibility of each class teacher, with the site moderated by the school principal, deputy principal and ICT Team.
- If any parent or guardian has any concern about the appropriateness of the content of the website or social media sites, then the Board of Management asks that the matter be brought to the attention of the Principal as a matter of urgency.
- This policy should be read in conjunction with our Data Protection Policy.
- The publication of student work will be coordinated by members of staff.
- The school will endeavour to use 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.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will endeavour to avoid publishing the first name and last name of individuals in/beside a photograph.
- Pupils will continue to own the copyright on any work published.

Personal Devices

For use of personal devices for educational purposes (Assistive Technology), please refer to Saint Augustine’s Bring Your Own Device (BYOD) policy.

Students are permitted to use their own devices on the buses to and from school, before school and with permission from staff. Students are expected to use these devices in accordance with school policy. Use of personal devices outside of these times, or misuse will lead to possible sanctions and/or removal of privilege of using personal devices on the buses or at school.

Pupils using their own technology in school without permission, 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 in direct breach of the school’s Acceptable Use Policy.

Students may not use any personal device to record or take images while in school or on a school outing. Any such breach of the Acceptable Use Policy (AUP) will be sanctioned accordingly.

Any personal devices are to be turned off during school hours.

Any images or recordings of students should be taken using school owned devices only (iPads, Class Cameras, etc.).

The student is responsible for keeping their device in their possession or properly securing it, at all times. St. Augustine’s is not responsible for the security or condition of student’s personal devices.

The student is responsible for the security of their devices they bring to school. It is always a good idea to record the device’s serial number to have in case of theft. St. Augustine’s is NOT responsible for the theft of a device, nor is the responsible for damage done to the device while at school. If theft occurs, you should contact a school administrator to make him/her aware of the situation.

The student must comply with the teachers’ request to refrain from using a device, verify/display the authentication login screen, or to power down (turn off) the device.

Violations may result in the loss of privilege to use personal technology in school or on the school buses, and/or disciplinary and legal action, as appropriate.

Support Structures

Staff, parents and students should familiarise themselves with up to date information and advice on internet use and safety. As the pace of technology is rapid and ever changing, regular use of the Webwise site is advocated.

- www.webwise.ie : A guide to safe internet usage for children.

There are other organisations who deal with internet safety and can prove to be a source of support for parents and teachers alike. These organisations can be accessed through the following sites:

- www.hotline.ie : Reporting illegal or harmful content on the internet.
- www.safekids.com : Family guide to internet safety.
- www.getnetwise.org : Safety, spam, privacy and security site.
- www.bernados.ie : Online Safety Program

When needed, the school will run a programme on acceptable internet usage for students/parents/guardians. This will cover several topics including cyber-bullying.

Staff will partake in Continuous Professional Development in relation to the development of AUPs, internet safety and cyberbullying.

The school will avail of additional expertise from outside agencies such as Garda Siochana, PDST, internet training providers, etc.

Sanctions

Misuse of the Internet or any activity which is in contravention with this Policy, may result in disciplinary action, including written warnings, withdrawal of access privileges, and, where appropriate, suspension or expulsion in line with the Code of Behaviour.

Staff Use of school ICT

- School Personnel should use the web for educational and professional purposes only during the school day.
- Equally School Personnel who are engaged in after school activities should restrict their use of the web to professional and educational purposes only while pupils are present.
- If a staff member wishes to access the web for personal purposes it should be done outside of pupil-teacher contact time.
- Any students on placement from the teacher training Colleges, transition year pupils or students on a work experience placement can only have access to the computer facilities under the supervision of the class teacher. Permission should be sought from the class teacher prior to use.
- Use of the internet by staff members to access inappropriate material whether it be pornographic, racist or offensive, is strictly prohibited at all times. No person will in any way alter the filtering preferences.
- Staff will be responsible for creating and using secure passwords for all accounts.

Legislation

There is no specific legislation governing Internet safety at school level. Complicating this issue is the fact that the Internet functions in a global context whereas the law operates in a localized one. There are, however, a number of legislations that have relevance to Internet safety. They are briefly described as follows:

- Data Protection (Amendment) Act 2003 www.dataprotection.ie

  This amendment extends the data protection rules to manually held records and also makes improvements to the public's right to access data.

- Child Trafficking and Pornography Act 1998 www.acts.ie

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

- Interception Act 1993 www.acts.ie

  The Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 stipulated that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.

- Video Recordings Act 1989 www.acts.ie

  This act prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer. It would apply where someone in the State supplied this kind of video over the Internet.

- The Data Protection Act 1988 www.dataprotection.ie

  This act was passed in order to deal with privacy issues arising from the increasing amount of information kept on a computer about individuals.

- Copyright and Related Rights Act 2000. The Law governing copyright in Ireland.
- EU General Data Protection Regulations 2018
- Anti-Bullying Guidelines for Primary Schools 2013

SIGNED: MARIAN COUGHLAN

CHAIRPERSON, BOARD OF MANAGEMENT

SIGNED: DAVID O’ BRIEN

SCHOOL PRINCIPAL

Date: 28/01/21 Date of next review:

St. Augustine’s School - Acceptable Use Policy

Permission Form

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

Name of Pupil: ________________________ **DOB:** ___________

Pupil

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

Pupil’s Signature: ______________________________ **Date**: ___________

Parent/Guardian

As the parent or legal guardian of the above pupil, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access ICT equipment and 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 pupils access unsuitable websites.

I accept the above paragraph □ **I do not accept the above paragraph** □

Parent/Guardian signature: ________________________ **Date**: ___________

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 children’s work on the school website.

I accept the above paragraph □ **I do not accept the above paragraph** □

Parent/Guardian signature: ________________________ **Date**: ___________