Scoil an Chroí Ró Naofa Íosa
(Sacred Heart of Jesus National School)
Huntstown
Dublin 15
D15 KF65

Teileafón: 01 8216400
Ríomhphost: sacredheartns@gmail.com
Suíomh Idirlíon: www.shns.ie
Uimhir Rolla: 19755L

ICT Acceptable Use Policy (ICT AUP)

Introduction

The aim of this ICT Acceptable Use Policy (ICTAUP) is to ensure that students benefit from learning opportunities arising from their use of the school's technology and internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school's ICTAUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, as outlined below, will be imposed.

The provision of ICT resources and access to the internet is for the express promotion of effective teaching and learning and is established in line with the principles for effective ICT education promoted by the Department of Education (D.E.).   The policy outlines the rights and responsibilities for all users. The aim of this policy is to give guidance and direction for the acceptable use of ICT for teaching and learning and communication as appropriate for all members of the school community, to include pupils, staff, parents, guardians and approved visitors/speakers who have access to, and are users of ICT.

It is envisaged that the ICT committee, together with staff, parents and the Board of Management will review this ICTAUP on a regular basis in response to emerging technologies and issues arising.

……………………………………………………………………………………………

School Strategy

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

General

- Internet sessions will always be supervised by a teacher in the school setting.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material. The National filtering protocols (HEAnet) established to safeguard schools from inappropriate content are adopted for use by the school. "Content filtering is an essential and integrated element of the broadband service that is provided to schools by the Schools Broadband Programme. The purpose of content filtering is to ensure (in so far as is possible) that inappropriate websites and content are not accessible from within schools" (PDST, Technology in Education). The HEAnet broadband filtering service is currently set at Level 4.
- Staff will monitor how and when students engage with online material.
- Students and teachers will be provided with training 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 where appropriate.

- The use of personal memory sticks, CD-ROMs, online or cloud storage facilities or other digital storage media by a student in school requires the permission of a staff member.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- ICT devices referenced in this policy include all technological equipment used for recording videos, images and audio as well as all devices used for communication and distribution of data including mobile and smart telephones, laptop computers, tablet computers, desktop computers, smart watches, smart glasses and internet dongle devices.

Use of ICT Devices in School

- Students are not permitted to use personal ICT devices such as mobile or smart telephones / smart watches / cameras / digital glasses / digital headsets / internet dongle devices or equivalents or other such video / audio / visual recording devices during the school day or when involved in out-of-school activities such as tours / trips or extra-curricular activities.
- Use of ICT devices in the school for educational purposes such as laptop computers, tablet computers, desktop computers, smart watches and all other technological devices will be determined by the school. All devices for use by students during school activities must be provided and approved by the school and are not permitted to be brought home by individual students at any time. Pupils will not use personal ICT devices during the school day or when involved in out-of-school activities such as tours / trips or extra-curricular activities.
- Assistive technologies – students who require the use of assistive technologies in school will be permitted to use those sanctioned by the N.C.S.E / D.E.
- Children will have access to the school landline or mobile telephone, under the supervision of a school staff member, in the case of an emergency. Children are not allowed use mobile phones on the school premises, i.e. in the school grounds or school building. All mobile phones must be switched off and kept out of sight. The school cannot accept responsibility for any loss or damage to mobile phones.
- During the school day, or whilst engaged in school activities, students are not permitted to:
  - make or receive phone-calls
  - send or receive text messages or any type of digital messages
  - make audio, video or photographic recordings.
- If a student uses a device during the school day, or whilst engaged in school activities, to engage in an activity as listed in the previous point he/she will receive a verbal warning on the first occasion and the device will be placed safely in storage until dismissal time. On a second or subsequent occasion, the device will be placed safely in storage until parent(s)/guardian(s) of the child retrieve it from the principal and/or the class teacher. If a device is repeatedly used in school, the matter may be dealt with, with reference to the school's Discipline and Code of Behaviour Policy. Associated sanctions may be employed.

World Wide Web

- Students will use the internet for educational purposes only and with the permission and under the supervision of, a member of the school staff.
- Students will not visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will be familiar with copyright issues relating to online learning.
- Students will not 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.
- Students will normally use child friendly search engines under the direction of staff (i.e. Kidrex, Kiddle etc).
- Students must report accidental accessing of any inappropriate sites or materials to a teacher immediately.
- Students will not upload or download digital content and will not be permitted to share digital content across the internet without the express permission and supervision of a member of the teaching staff.
- Students will endeavour to download and use images, videos and all other materials that are copyright compliant and will not publish or share material that might cause a breach of copyright law. Safe searching through sites such as 'Creative Commons' will be promoted and encouraged.
- Students are not permitted to access the internet from a preconfigured private 'hotspot' connection such as through a mobile telephone service provider.

Email

- Students will not be permitted to access personal email addresses while in school.
- In the promotion of safe email practices at home, students will be reminded:
  - ✓ Not to send or receive any material that is illegal, obscene and defamatory or that is intended to annoy or intimidate another person.
  - ✓ Not to reveal their own or other people's personal details, such as addresses, telephone numbers or pictures.
  - ✓ Never to arrange a face-to-face meeting with someone they only know through emails or the internet.
- Teachers may only access personal e-mail accounts outside of teaching hours. Teachers must ensure that e-mails accessed are appropriate for a school setting and must not open any e-mails that they suspect may contain any virus or inappropriate material. The use of personal e-mail accounts during student contact time should be for educational purposes only.
- Teachers will endeavour to use internal online services such as Aladdin or its approved equivalents to communicate messages to other staff members.

File Sharing and Distribution of Media

- Students are strictly prohibited from sharing images, videos, audio or other online content which may be deemed harmful to another member of the school community.

- While on school grounds or when participating in school activities, students are only permitted to take photographs, videos and audio recordings using school based and teacher approved devices with express teacher permission. These recordings remain in the school's ownership and may not be shared or distributed without the full permission of the teacher.
- Excepting when students have teacher permission to use school based and teacher approved devices to make a recording, there are no other circumstances where students may take, use, publish or distribute images, video or audio recordings of any member of the school community while involved in school related activities, including extra-curricular sports and off-campus activities.
- It is the responsibility of parents / guardians to ensure their child / children adhere to relevant terms of service agreements pertaining to data sharing technologies so that they do not share images, video or audio recordings of any member of the school community without their permission or share images, video or audio recordings which might be deemed invasive, offensive or defamatory. Students should not comment on, or make reference to, a member of staff on digital communication or social media platforms. Students should not circulate or publish, through ICT or other means, material recorded without consent that may undermine, or cause damage to, the professional or personal reputation of another person. Any breach of these rules may be dealt with, with reference to the school's Discipline and Code of Behaviour Policy. Associated sanctions may be employed.
- Where YouTube and other video sharing sites are used in school, staff will evaluate, approve and monitor the content to be shown to students.

School Website

- Students will be given opportunities to publish teacher-approved projects, artwork or school work online.
- 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 express written permission.
- Where images / videos / audio of students are included on the school website, full personal details (e.g. first and second names together) will not be attributed to such recordings.
- Personal student information including home address and contact details will be omitted from school web pages.
- Students will continue to own the copyright on any work published.
- Students are not permitted to publish material on the website that breaches plagiarism rules and may only have material published that is uniquely their own.
- The school website and domain name remain in school ownership and content may only be updated to the site by staff members.
- The school website and Twitter accounts are for the purposes of disseminating information on school activities and events to the wider school community. They are not a vehicle for gathering or sharing opinions.

Social Media and Web 2.0

- Students must not use social media, messaging applications, gaming devices or the internet in any way to harass, insult, abuse or defame students, their family members, school staff or their family members or other members of the school community.
- Students / Parents / Guardians should never attempt to contact any member of school staff using social media or online means. Where online platforms such as Aladdin / Seesaw or their equivalents are sanctioned for use by the school as a means of communication, students / parents / guardians must use them appropriately and should always endeavour to be courteous and respectful in their communications with staff.
- Students are not permitted to share personal information about students, staff and other members of the school community social media, messaging applications, gaming devices or the internet.
- Students must adhere to the terms of service of all instant messaging services and applications including Snapchat, WhatsApp, Viber, Facebook, Instagram, TikTok and their equivalents and comply rigorously with the digital age of consent.
- Students are permitted to use blogs and website creators such as Word Press and Weebly when it is for educational purposes. This is permitted under the guidance and permission of staff. All codes, passwords and access material pertaining to these blogs and websites remain under the control of the school.
- Access to video streaming sites such as YouTube and Vimeo etc. is allowed for educational purposes only with guidance and permission of school staff.
- Students must not engage in activities involving social media or any form of communications technology, which might bring the school into disrepute or defame students, staff or the wider school community.
- School / Class Dojo accounts or their equivalents will be closely monitored and controlled by staff members and will not be used as a primary means of communication between school and home. Portfolio sharing facilities such as 'Seesaw' and its equivalents will be used prudently and judiciously by staff. Due diligence will be exercised in the collection, retention and distribution of work samples. Access codes and passwords will be protected. Due diligence will be exercised in the collection of data such as images and audio to ensure that the identity of individual students is not widely distributed and shared.

Distance and Virtual Learning Experiences

In the event of a prolonged school closure (e.g. owing to a Public Health pandemic), where students and staff are directed to work remotely, the school will make every effort to use technology in a safe and careful manner. Actions and interactions through online platforms and the behaviour of students, families and staff will be informed and governed by the school's Child Safeguarding Statement and Child Safeguarding Policy. To this end the following provisions are in place:

- Communications with families will be through Aladdin Connect or an equivalent platform which has been approved for use by the school.
- Where staff members use email to contact families, the staff members' personal email addresses will not be used.
- Concerns regarding child safety, identified during distance learning experiences, will be reported to the Designated Liaison Person.

- When sharing material with families, staff will pre-record lessons, instructions, work samples and videos using a variety of recording tools. Staff will also judiciously use educational content from external sources and only direct students / parents / guardians to content that they have evaluated to be appropriate for the specific educational context.
- Where staff shares pre-recorded lessons or instructions using online facilities parents, guardians and students agree to treat these recordings with respect. They will not be altered, edited or distributed without the express permission of the staff member and the staff member retains copyright ownership on all pre-recorded lessons and content.

Legislation

The school directs parents to the following legislation for further information on the use of the internet:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 2018
- Copyright and Related Rights Act 2000 – this act governs copyright in Ireland.
- Anti-Bullying Guidelines for Primary Schools 2013
- GDPR 2018

GDPR

On May 25th 2018 the introduction of GDPR and the adopting of 16 as the Digital Age of Consent in Ireland came into effect. The Digital Age of Consent is the minimum age a user must be before social media and internet companies can collect, process and store their data. The E.U. has set the Digital Age of Consent to 16 by default. The Digital Age of Consent refers to the age at which young people may sign up for online services, such as social media sites, without needing the explicit approval of their parent or guardian. It is the obligation of parents / guardians to safeguard their children from inappropriate online participation and students must not sign up for accounts such as Instagram, Snapchat, Facebook, Twitter, WhatsApp, TikTok or their equivalents if in doing so is in contravention to the Digital Age of Consent. They must abide by the agreed terms of service pertaining to these social media platforms. Students who contravene the Digital Age of Consent do so at great personal risk and parents / guardians should ensure that their child is fully compliant with same.

Scoil an Chroí Ró Naofa Íosa is a controller of personal data relating to its past, present and future staff, students, parents / guardians and other members of the school community. The school endeavours to abide by GDPR regulations in the following manner:

- Obtaining and processing personal data fairly and securely
- Keeping such data for specific and lawful purposes
- Maintaining all personal data safe and secure so that it cannot be accessed by unauthorised third parties. Password protected computers and restricted access to data is promoted throughout the school.
- Maintaining accurate and complete personal data which is regularly updated.

- Insisting that data collected is appropriate, pertinent and justifiable.
- Retaining it no longer than is necessary for the specified purpose or purposes for which it was given.
- Making their data available to individuals upon request.

Further information on data protection rights and responsibilities can be found in the school's Data Protection Policy.

Support Structures and Internet Safety promotion

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the internet e.g. www.hotline.ie and www.webwise.ie.

Provisions to promote internet safety and ICT awareness will include:

- The delivery of internet safety lessons as part of the SPHE curriculum. These lessons are delivered throughout the school year as part of the SPHE curriculum. This includes but is not limited to Stay Safe Lessons, 'Barefoot Computing Internet Safety Resources' and My Selfie / Webwise resources.
- As part of the school's Anti Bullying Awareness Initiative, workshops for pupils on Online Safety and Cyber Bullying are organised for pupils and parents on a regular basis.
- An internet safety week which includes a school wide promotion of internet safety and ICT competency, delivered annually at an agreed point on the school calendar.
- School staff will be provided with continuing professional development in the area of internet safety and online communication and ICT technologies. This may involve but is not limited to: the invitation to the school of internet safety speakers, in-school workshops and tutorials provided by suitably qualified staff.

ICTAUP and Parents / Guardians and the School Community

- Under E.U. law (GDPR), the Digital Age of Consent is 16 years of age. In the interest of the child's welfare, it is the responsibility of parents / guardians to ensure that their child abides by the Digital Age of Consent with respect to all social media platforms, messaging services and online platforms such as Instagram, Snapchat, Facebook, Twitter, WhatsApp, TikTok and their equivalents.
- The welfare of the student – their emotional and mental wellbeing – should inform and guide the parent / guardian in how s/he/they allows their child to access online content.
- It is the responsibility of parents / guardians to control the type and nature of personal devices that their child may access.
- The publication of videos, images, audio or other media taken by visitors to the school is prohibited on all social media platforms and digital sharing services.
- Parents / Guardians must not use any digital device (such as a mobile telephone, smart watch, iPad etc.) to make audio or visual recordings of staff members while they are engaged in their professional duties in school, on the playground / yards or while working with students outside of the school grounds (e.g. on a school trip / outing or at a sporting event).

- Parents / Guardians are not permitted to capture, use, share, publish or distribute recordings (image / video / audio) of any member of the school community without their permission.
- Activities conducted online involving social media by parents / guardians must not defame the school or bring it into disrepute. All personal opinions expressed online are those of the parent / guardian and are not to be attributed to the school.
- Parents / Guardians who use social media or the internet must not harass, insult, abuse or defame pupils, their family members, staff or other members of the school community. Serious transgressions may be brought to the attention of the Board of Management and/or other relevant external agencies.

ICTAUP and the Parents' Association

- The Parents' Association will not advertise inappropriate products or services on Facebook / Twitter or other social media platforms.
- The Parents' Association will not post any comments or information that could be deemed as offensive, inappropriate, harmful, or contrary to school ethos or policy.
- The Parents' Association must not post or tag images of pupils or staff members on social media platforms.
- The Parents' Association must not accept pupils as users or links on Facebook pages or other social media platforms.
- The Parents' Association social media platforms must not be used as a discussion forum about pupils, staff or school policies etc.
- Blogs or social media services used to disseminate information must not be a vehicle for publishing or distributing images of any member of the school community without their permission and should not defame or impugn the good name and reputation of any student, staff member, parent / guardian or member of the school community.
- Social media platforms used by the Parents' Association must be honourable, fair and reasonable in their presentation of information to parents.

ICTAUP and Teachers, Staff and Visiting Agencies

- Staff members will access and use ICT resources including the internet paying close attention to the principles for good practice and professional standards outlined by the Teaching Council (Code of Professional Conduct for Teachers, 2016).
- Staff should be guided and informed by the guidelines for accessing and using social media, outlined by the Teaching Council (digital copy available at: https://www.teachingcouncil.ie/en/publications/fitness-to-teach/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.pdf).
- Staff will seek parent/guardian permission before publishing images / videos of students on school websites / blogs / digital sharing platforms.
- Visiting agencies such as occupational therapists, speech and language therapists and all other educational and support staff who visit the school may not make recordings of students or staff without the full permission of the school and parents / guardians.
- Staff members who use social media or the internet must not harass, insult, abuse or defame pupils, their family members, staff or other members of the school community.

- Staff members and authorised school visitors / agencies must not engage in activities involving social media or any form of communications technology which might bring the school into disrepute or post material or content which might defame or impugn any member of the school community.
- Staff members are not permitted to use, share, publish or distribute images of any member of the school community without their permission.
- Staff members using the internet and ICT resources with students as part of teaching and learning are required to supervise and monitor the behaviour of all students. Online material must be previewed and approved by staff as being appropriate, before it is shared with students.
- Staff members will ensure that school WiFi, Aladdin Pupil Management System and network administrator passwords are not disclosed to pupils or non-staff members.
- Use of the internet by staff members or authorised school visitors / agencies to access or download offensive or inappropriate material is strictly prohibited at all times.
- The HEAnet school broadband filtering level is approved by the Board of Management and must not be altered or amended by the staff. Decisions to change the broadband filtering level will be made by the Board of Management.
- Staff members may access the internet for personal purposes outside of pupil-teacher contact time only.
- Teaching practice students, transition year students or adults or students on a work experience / placement may only access ICT facilities with the permission of their mentor or supervising class teacher.
- All teaching practice and placement students must adhere to the ICTAUP and acceptance of a teaching placement for any duration requires that the student adheres to all aspects of the ICTAUP both in school and in the preparation of material outside of school.
- Staff members will only use school digital cameras and school iPads / school Chromebooks / other approved ICT equipment for the recording of images, videos and audio recordings of students for school related purposes.
- Content collected digitally by staff will be managed and controlled with due diligence and care. Where portfolios or online platforms are used, staff will exercise caution in the selection, publication and management of these files.
- Staff members and authorised school visitors / agencies must not post or share personal information, use, share, publish or distribute audio or visual recordings of students, staff and other members of the school community on any personal social media accounts or instant messaging services.
- Opinions expressed by staff members or visitors / agencies online are expressly those of the individual and must not be attributed to the school.
- All staff members should take appropriate measures to manage their online privacy and professional reputation while engaging with social media on a personal basis. Teachers will abide by the standards for good practice established by the Teaching Council.
- Staff members will never seek to connect with any student online using social media or instant messaging services.
- Teachers may not use mobile telephones during contact time with students except in exceptional circumstances. Teachers may require the use of personal mobile telephones as part of organisational matters such as coordinating school outings, sporting events or liaising with educational support services but this will be reserved for non-contact time with students. This may also involve accessing online services to complete attendance registers. This professional use of mobile telephones demands that the

teacher acts fairly and in the best interests of the students and wider school community and is permissible in exceptional circumstances only. All other use of mobile telephones will be restricted to non-contact time.

- Teachers may only access personal e-mail accounts outside of teaching hours. Teachers must ensure that e-mails accessed are appropriate for a school setting and must not open any e-mails that they suspect may contain any virus or inappropriate material. The use of personal e-mail accounts during student contact time should be for educational purposes only.

- Teachers are only permitted to utilise school printing resources for personal use in exceptional circumstances and then only in a limited manner. If a teacher wishes to utilise school resources to print personal material they must first seek permission from the Principal or Deputy Principal.

Sanctions

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension in line with school discipline policy. The school also reserves the right to report any illegal activities to the appropriate authorities including the Gardaí, Tusla and the Office of the Data Commissioner.