Cork Educate Together Secondary School

Internet and ICT Acceptable Usage Policy (AUP) 2.0 January 2021

CETSS offers parents the choice of an education based on the inclusive intercultural values of respect for difference and justice and equality for all. In our school, every child will learn in an inclusive, democratic, co-educational setting that is committed to enabling and supporting each child to achieve their full potential while at the same time preparing them to become caring and active members of a culturally diverse society.

Adapted from Educate Together Mission Statement

Introduction

CETSS recognises that access to Information and Communication Technology (ICT) gives our students enhanced opportunities to develop skills that will equip them for 21st century life. For this reason, CETSS provides access to ICT for student use. This Acceptable Use Policy outlines the guidelines and behaviours that our students are expected to follow when using school technologies or when using personally owned devices inside CETSS campus or at CETSS organised events.

Technologies Covered

CETSS may provide students with internet access, access to desktop computers, digital imaging equipment, laptop or tablet devices, video-conferencing capabilities, virtual learning environments, online collaboration capabilities, online discussion forums, apps, email and more. As new technologies emerge, CETSS may provide access to them also. During school closures CETSS may also provide access to remote learning via online lessons and meetings via Zoom, WebEx, Teams, or other similar apps. WebEx should be favoured for in-school business where at all possible. The policies outlined in this document are intended to cover all online and offline technologies used in the school, not just those specifically mentioned. As new technologies are incorporated into CETSS, this policy may be updated accordingly.

CETSS ICT Network

CETSS computer network is intended for educational purposes. Access to ICT is considered a school resource and a privilege. Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, as outlined in this AUP, will be imposed.

● 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 policies of the Department of Education and Skills through its agency, the National Centre for Technology in Education.

● Students are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the web at school. If a site is blocked and a student believes it shouldn't be, the student can ask his/her teacher to submit the site for review.

● Proxy servers (eg VPN, hot-spotting) are strictly forbidden. Any attempt to circumvent the internet filtering system is a serious breach of this AUP and will result in confiscation and/or sanctions.

● Students should not engage in any activity online which is in breach of local, national or international law.

● Students should not engage in any activity which may bring CETSS, its staff or student body into disrepute.

● Students are expected to follow the same rules for good behaviour and respectful conduct online as offline – these rules are found in CETSS's Code of Positive Behaviour.

● Misuse of school resources and/or online lessons and meetings may result in disciplinary action.

● We make a reasonable effort 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/platforms.

● A student is expected to alert his/her teacher immediately of any concerns for safety or security.

CETSS email and online collaboration

CETSS provides students with Office 365 accounts for the purpose of school related communication and work. Availability and use is restricted in line with school policies. Office 365 accounts should be used with care. Email and/or other Office 365 app usage may be monitored and archived. CETSS recognises that online collaboration is essential to education and may provide students with access to a variety of online tools that allow communication, sharing, and messaging among students. Students are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline. All messaging on school platforms is expected to be school-related.

CETSS Security

Students are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes, but is not limited to, not opening or distributing infected files or programmes and not opening files or programmes of unknown or untrusted origin. Students are expected to use common sense: if student thinks a website does not look right he/she must inform a teacher. If a student believes a computer or mobile device might be infected with a virus he/she must alert a teacher (in school) or a parent/guardian (at home). Student should not attempt to remove the virus him/herself or download any programmes to help remove the virus. Students should not download or attempt to download or run .exe programmes over the school network or onto school resources. Students may be permitted to download other file types, such as images or videos. For the security of the school network, such files should only be downloaded from reputable sites and only for educational purposes. Any student-use of a USB or other storage device must be by agreement with the teacher/staff-member and the student must be certain there is no virus transmission via the connected device.

Netiquette

Netiquette may be defined as 'appropriate social behaviour over computer networks and in particular in the online environment'.

To this end:

● Students should always use the internet, network resources, and online sites in a courteous and respectful manner. This includes the use of their proper name rather than pseudonyms and profile picture/avatar which is not offensive to the school ethos.

● Students must use their school-provided resources (eg Office 365 email, Schoology messaging, Schoology groups, etc) for all school-related contacts/assignments/projects/groups and not personal e-mail. This includes contacting staff or students

● The internet should be used for educational purposes only.

● Students should also recognise that in addition to the valuable content online, there is often unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the internet.

● Students should not post anything online that they wouldn't want parents, teachers, or future colleges or employers to see.

Plagiarism

● Students should not plagiarise (copy or use as your own without citing the original creator) content, including words, code or images, from the internet.

● Students should not take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online. Research conducted via the internet should be appropriately cited, giving credit to the original author.

● The school may check for plagiarism using online tools.

Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety or the safety of others, bring it to the immediate attention of:

● a teacher if you are at school.

● a parent / guardian if you are at home.

● Students should never share personal information about themselves or others, including phone numbers, addresses, PPS numbers and birth-dates over the internet without adult permission. Any breach of this will be seen as a serious breach of school rules and will carry with it appropriate sanctions.

● Students should never agree to meet someone they meet online in real life without parental permission.

● Student profiles created online (Schoology for example) must be accurate, educational and not mis-used. Any uploaded image (photo or otherwise) must be appropriate.

● Students must not remove/alter iPad management software or remove/alter parental controls set-up by parents, Wriggle and/or school on their devices.

Cyber-bullying

The Department of Education and Skills defines cyberbullying as; "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." Harassing, 'flaming', denigrating, impersonating, outing, tricking, excluding and cyber-stalking are all examples of cyber-bullying.

● Such bullying will not be tolerated in CETSS. See CETSS's Anti-bullying Policy.
● Inappropriate actions on social media sites can also constitute bullying, e.g. "liking" degrading comments/photos on Facebook, Trolling etc.
● Don't be mean. Don't send emails or post comments or photos with the intent of scaring, hurting, or intimidating someone else.
● Engaging in any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action and loss of ICT privileges.
● In some cases cyber-bullying is a crime and may be reported to the Garda.
● Students are advised that activities are monitored and retained.
● The school will support students, teachers and parents in dealing with cyber-bullying.

Violations of this Acceptable Use Policy

Violations of this policy in CETSS may have disciplinary repercussions including but not limited to:

● Suspension of network and computer privileges
● Temporary confiscation of device
    ● this may involve the device being handed over to the authorities for further investigation. CETSS reserves the right to report any illegal activities to the appropriate authorities
● Temporary limitation of device.
    ● including removal of browser access, apps, games, social-media etc.
● Notification to parents
● Community Action
● Suspension from school and/or school-related activities
● Expulsion
● Legal action and/or prosecution

Date of Ratification:

To be Reviewed in 2022

XXXXXXXX   Colm O Connor

Chairperson of the Board   **Principal**

_____   _____

AUP addition - Remote Learning during the Covid-19 Pandemic

This section sets out guidelines and information to students, their parents, and staff, surrounding the use of technology when learning remotely i.e. from a place other than school and where it is not possible for the teacher to deliver the class within the same location, as would be the case, if the class was taking place in a classroom setting.

This section is informed by Tusla's Considerations for Safeguarding children and young people when providing online lessons and 'Guidance on Continuity of Schooling' for teachers which is available on the Department of Education's website
https://www.education.ie/en/SchoolsColleges/Information/guidance-on-continuity-ofschooling.pdf

The Professional Development Service for Teachers (PDST) have created a short one-hour course aimed at helping teachers to teach and support online learning. This is referenced in the above document and a link to the same is provided on their website.

The agreed online platforms our school is currently using are Office 365 which includes outlook email and Teams - including meetings feature – and Schoology. When students are remote learning the Code of Behaviour still applies.

1. All software including operating systems and anti-virus software must be up to date if teachers or students are using their own devices rather than school devices to login into our system.
2. Students should follow the distance learning timetable as best they can. Teachers will be available online to answer questions and discuss issues with students – the ideal way for students to reach them is via Schoology Messaging. Teachers may email work to students for the student to complete, deliver a live class using Teams (or similar app), set tasks on Schoology, or set other online/offline work which is later submitted via Schoology.
3. Attendance may taken by the teacher and shared using tracking spreadsheet. This would be monitored and communication is made with parents based on this information. All non-compliance with work/tasks/assignments will be recorded on VSware and followed-up by the Deputy or appointed other staff. Attendance is mandatory (just like when school is open) and all absences must be declared/excused by parents.
4. Provision for AEN students will be made in agreement with the parent and student.
5. Care should be taken to ensure the lessons are age and developmentally appropriate and that thought is given to the amount of screen time needed to participate.
6. Teachers may use MS Teams (Zoom, Webex or similar agreed apps - WebEx should be favoured for in-school business where at all possible) to livestream classes, teach remotely, or share audio/video recordings. In line with TUI guidelines, teachers will not share recordings of lessons. Recordings must not be made of any online classes, tutor time or assemblies. ~~other than by the teacher unless with explicit agree from the teacher~~. Such recordings by the teacher are not permitted to be shared with anyone or by anyone other than by the teacher. In the case of remote learning, teachers will trust students to behave appropriately online, as they would in their real classroom. The teacher will stay on an online meeting call until all students have left. If the teacher loses the connection and can't reconnect, the Principal or Deputy will join and end the call. Students are not permitted to share the link with anyone else.
7. Teachers may record the lesson in order that students can use it for revision purposes, or those who cannot make the live lesson can access it. This will not be shared with students.

Teachers must let the students know that they are recording. These videos are not to be shared outside of Office 365 and are for CETSS use only.

8. During remote learning teachers will design learning experiences that encourage students to work together, this will involve students communicating with each other. When working in groups, teachers will give clear guidance on how students should communicate on their task. For example, students should use teams, ~~seesaw~~, Flipgrid, the collaboration space on OneNote, or Sharepoint on Office 365, or Schoology (or other Whitelisted Apps) to communicate with each other. When working individually students wishing to communicate with their classmates should use the posts section on teams or their school email or Schoology. If students wish to communicate with their teachers, they must use their school email or the posts section on teams or Schoology messaging. Teachers will not reply to external email addresses.

9. Teachers and students' attire must be suitable if the video feature is being used. Teachers and students are asked to be aware of their background when using the video feature, ensuring it is appropriate. Students are not obliged to turn the video feature on, but we encourage them to turn on their video to help create a sense of community. Students must keep the same icon also so that they can be easily recognised by their teacher.

10. A teacher will only correspond with a student on our Microsoft platform. A teacher will only correspond and engage with a student who is using and is logged into their school account. All student questions are to be posted on Teams or Schoology only. Teams chat function may also be used between teacher and student, chat between student and student is only permitted with teacher permission and must be work-related. In limited circumstances a teacher may request permission from the DP/P to hold a meeting on another platform eg: zoom. Students will be asked to join a meeting on another platform by clicking on a link which will be sent through their Teams Platform. This will be rare and will usually involve an external speaker who does not have access to our Microsoft Platform. The teacher will be present for the online meeting and the same guidelines apply as if the meeting was on our Teams Platform. Students are not permitted to share the link to that meeting.

11. For reasons of Child Protection and GDPR, parents/guardians/third-parties are requested not to participate in online classes. However, if they have a query or suggestion, they are welcome to email the school and it will be forwarded to the teacher of the subject. In line with school policy and normal classroom procedures, almost all requests for feedback/queries should come from students via the traditional channels.
    a. A student enabling a 3rd party to enter an online teaching/meeting space will be considered a very serious breach of the school code of behaviour. In particular, if this exposes other students and staff to inappropriate/lewd/indecent/insulting/bullying behaviour, it will be considered a level 5 incident.

12. Use of personal social media accounts e.g. Facebook, Snapchat, Instagram, WhatsApp etc, to communicate with students is never permissible and teachers have been advised accordingly.

13. Any behaviour or language deemed inappropriate during school also applies during online learning. The consequences for such behaviour will be the same as if the student was in school - as much as is possible if the school is closed/partially closed.

14. All provisions relating to the child's data remain the same under GDPR procedures and guidelines.

15. School Office 365 accounts are to be used for school related purposes only.

16. It is expected that all students and teachers will engage as best they can with all efforts at online teaching and learning so as not to be behind when normal school resumes. Make sure

your teacher (or SNA, or Guidance/SENCO/DP) knows if you are feeling overwhelmed with the amount of work. It is ok for this to feel different to normal school life.

17. Students are frequently reminded to contact their tutor, DP or principal by email if they have any concerns or issues.

18. Students and parents will be issued with guidelines and procedures for live online lessons/meetings in case of any school closures. These will be reviewed from time to time and issued in advance of online lessons/meetings via the school App.

19. One-to-one teaching online (support-space scenarios, during lockdown or similar situation) should not occur. A second adult is required 'in the room'. This could be another teacher or an SNA.