

School Name: Scariff Community College

Address: Drewsborough, Scariff, Co. Clare V94 Y9W2

The aim of this Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's digital resources in a safe and effective manner. The responsible use of internet and digital technologies, both online and offline and access considered an integral part of teaching and learning. Therefore, if the school AUP is not adhered to agreed sanctions will be imposed.

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

This version of the AUP was created on _____ and ratified on _____.

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

- Filtering software _____ will be used in order to minimise the risk of exposure to inappropriate material
- Internet use in school is by permission of teacher
- Scariff Community College will regularly monitor student's internet usage
- Students will be provided with training in the area of internet safety
- Uploading and downloading of non-approved software is not permitted
- Virus protection software will be used and updated on a regular basis
- The use of personal external digital storage media in school, requires a teacher's permission. This includes but is not confined to memory sticks etc
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute

Internet Use

- 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 school devices, their school Microsoft Office 365 account and the internet for educational purposes only

- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement)
- Students will never disclose or publicise personal information or passwords
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's Acceptable Use Policy
- Students will be aware that any usage of the internet and school's digital platform, including distributing or receiving information, school-related or personal will be monitored

Email

- Student will use approved school email accounts
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy, harass 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 or the internet
- Students will note that sending and receiving emails attachments is subject to permission from their teacher
- Students will not forward email messages or screenshots or emails or "reply all" without the permission of the originator
- Students must only use their school email for school related activities and for registering on school-based activities only. The use of personal email addresses is not allowed for school-based work.
- Students should not use school email accounts to register for online services, social networking, apps or games
- Students should report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Students should report any such communications to a teacher
- Students should avoid opening emails that appear suspicious. Students should report any suspicious emails to a teacher
- All emails and opinions expressed in email are the responsibility of the author and do not reflect the opinion of the school

Social Media and messaging services for Staff and Students

- All members of the school community must not use social media, messaging services and the internet in any way to harass, impersonate, insult, abuse or defame others
- Staff and students must not discuss personal information about students, staff and other members of the school community on social media
- Staff and students must not use school email addresses for setting up personal social media accounts or to communicate through such media

- Staff and students must not engage in activities involving social media which might bring the school into disrepute
- Staff and students must not represent their personal views as those of the school on any social media service or message services
- Students will be provided with guidance on etiquette regarding social media. This includes junior classes completing an internet safety module based on web wise internet safety programme

Guidance for Teachers

Scariff Community College directs staff to Guidance for Registered Teachers about the use of Social Media and Electronic Communication here:

Digital Learning Platforms

- Scariff Community College digital learning platform operates using Microsoft 365
- Scariff Community College learning platform is owned and managed by LCETB. Microsoft 365 platform enable two-way communication
- Prior acceptance from parent representatives should be sought for student usage of the schools digital learning platform
- Use of email accounts as per Microsoft platform
- Only school platforms should be used for the purpose of capturing and storing media unless otherwise directed by the teacher
- All school related media and data should be stored on the Microsoft 365 platform
- The use of digital platforms should be used in line with considerations set out in the school's data protection plan (GDPR)
- Each user of the platform should have their own unique login credentials. Personal email addresses should not be used when creating accounts on school digital platforms
- Passwords for digital platforms and accounts should not be shared

Images and Video

- Care should be taken when taking photographic or video images that students are not identifiable
- Care should be taken when taking photographic or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students and staff must not take, use, share, publish or distribute images of others without their permission
- Students taking photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from a staff member

- Students and staff must not take or share images, videos or other content online with the intention to harm another member of the school community regardless of whether this happens in school or outside
- Sharing explicit images and in particular explicit images of students and/ or minors is unacceptable, illegal and absolutely prohibited behaviour, with serious consequences and sanction for those involved. Sharing explicit images of other students will involve sanctions up to and including suspension, and may be reported to the appropriate authorities

Communications Use of Personal Devices and School Website

Staff and students should be aware of the following regulations relating to the use of communication technologies by students

Communication Technology	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Personal devices may be brought to school	✓			
Use of personal devices in lessons			✓	
Use of personal devices on social time				✓
Taking photos on personal devices			✓	
Use of hand-held devices			✓	
Use of personals email address in school or on school network				✓
Use of school email for personal emails				✓
Use of chat rooms			✓	
Use of instant messaging			✓	
Use of social media sites and online forums				✓

Use of blogs				✓
--------------	--	--	--	---

Inappropriate Activities

Staff and Students should not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposal or comments that contain or relate to:

- Promotion or conduct of illegal acts e.g. under the child protection, obscenity, computer
- Misuse and fraud legislation
- Racist material
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Harmful content or threatening behaviour, including 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 or brings the school into disrepute
- Using school system to run a private business
- Use systems, application, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume networking traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- Online gaming
- Online gambling
- Online shopping
- Use of social networking sites, instant messaging and online forums
- Child sexual abuse material
- Any other activity considered questionable

School Website

- Students may be given the opportunity to publish projects, artwork or school work on the internet in accordance with clear policies and approval process 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 students or staff

- The publication of student work will be coordinated by a teacher
- The school will endeavor to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will only be published on the school website with parental permission
- Personal student information including home address and contact details will be omitted from school web pages
- The school website will avoid publishing the first name and last name of individuals in a photograph
- The school will ensure that the image files are appropriately named and will not use student's names in image file names ALT tags if published online

Cyberbullying

Bullying is unwanted negative behaviors, verbal, psychological or physical, conducted by an individual or group against another person (or persons) which is repeated over time". (Anti-bullying Procedure, Department of Education, 2013)

This definition also includes:

- Deliberate exclusion, malicious gossip and other forms of relational bullying
- Identity-based bullying including but not limited to 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

Department of Education Anti-Bullying Procedure, 2013 defines cyberbullying as "placing a once off offensive or hurtful public message, image or statement on a social network site or another public forum where that message, image or statement can be viewed and/or repeated by another people will be regarded as bullying behavior"

In accordance with the Anti-Bullying procedures for Schools; 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 behavior and our relevant school policies will be invoked.

Personal Devices

Student using their own technology in school should follow the rules set out in this agreement. They will only use personal devices (smartphone, tablet, smartwatch etc) in school under the direction and/or supervision of a teacher if they have permission.

Legislation

The school advises all stakeholders to familiarize themselves with:

- Data Protection Acts 1988 to 2018 and General Data Protection Regulations (GDPR)
- Copyright and Related Rights Act 2000
- Child Trafficking and Pornography Act 1998 and Criminal Law (Sexual Offences) Act 2017

- Children First Act 2015
- Harassment, Harmful Communications and Related Offences Act (Coco’s Law)
- Criminal Damage Act 1991

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 if the need arises.

Sanctions

Misuse of the internet and digital technologies will result in disciplinary action, up to and including suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Siochana.

Permission Form

Please review the attached school Acceptable Use Policy and sign and return this permission form to the Principal/ Year Head/ Class Tutor.

School Name: Scariff Community College

Name of Student: _____

Class/Year: _____

Student

I agree to follow the school’s Acceptable Use Policy on the use of the internet and digital technologies. I will use the internet and digital technologies in a responsible way and obey all the procedures outlined in the policy. I agree to using SCC digital Microsoft 365 platform.

Students Signature: _____ Date: _____

Parent/ Guardian

DRAFT