St. Joseph’s Grammar School

Scoil Iósaef

Social Media Acceptable Use Policy- Students

Policy Author	Ms D Dolan Head of ICT/ UICT Co-ordinator
Frequency of Review	Bi-Annual
Date of Last Review	June 2019
Date Approved by Governors	June 2021
Proposed by	
Seconded by	
Date of Next Review	June 2023

Introduction

St. Joseph's Grammar School recognises that access to school Social Media account(s) (and future emerging social media networks) gives pupils and staff greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping pupils develop 21st-Century technology and communication skills.

To that end, we provide access to technologies for pupil and staff use. This Social Media Acceptable Use Policy outlines the guidelines and behaviours that users are expected to follow when interacting with any school Social Media accounts, including via: 'hashtagging'; linking to a school account using the '@' sign eg. '@SJS41'; sharing; making mention of, via direct quotes or through Tweets modified in any way ('MT'); quoting (including direct/edited screenshots); 'DM' (direct messaging); 'retweeting' or making a Tweet a 'favourite'.

School Social Media accounts are ***intended for educational purposes***.

- ❖ All activity over Social Media may be monitored and retained.
- ❖ Pupils are expected to follow the same rules for good behaviour and respectful conduct on Social Media as offline.
- ❖ Misuse involving school Social Media accounts or any accounts either 'following' or being 'followed' by a school Social Media account can result in school sanctions being applied.
- ❖ We make a reasonable effort to ensure pupils' safety and security online, but will not be held accountable for any harm or damages that result from misuse of a school Social Media account.
- ❖ Student users of Social Media and followers of a school Social Media account are expected to alert **Mrs A McGleenan (Pastoral VP)** or **Ms D Dolan (ESafety Coordinator) immediately** of any concerns for safety or security.

Technologies Covered

St. Joseph's Grammar School currently provides internet access, desktop computers, mobile devices, video conferencing capabilities, online collaboration capabilities, message boards, email, and more that facilitates the use of and access to the Social Media service. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

As the nature of courses changed and coursework was introduced to more subjects there was a need to access resources via a digital platform such as My-School, Google Classroom and OneNote. With the migration to blended learning teaching staff may require students to access resources digitally via their smartphone. All access will be in line with the School BYOD policy needed to extend beyond Sixth Form.

St. Joseph's Grammar School recognise the benefits to learning from offering **all pupils** the opportunity to use personal ICT devices in school to support learners and their learning. It is the intention of this policy to facilitate and support the use of personal ICT devices i.e. smartphones, tablets, notebooks and laptops in school in furthering individualised student learning.

Usage Policies

All Social Media accounts established by the school are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Access

St. Joseph's Grammar School ***does not provide its pupils with access to Social Media during school hours.*** That access is restricted in line with safeguarding practices, C2K filtering and school policy. Students can see Twitter notifications on their My-School Home page and can view both the Facebook and Twitter feeds via the school website.

Browsing of Social Media during normal operative school hours is prohibited. Pupils are expected to respect that the restriction of access to Social Media on school grounds is a safety precaution, and should not try to circumvent it when accessing the internet at any point during the school day. This is clearly set out in the **Students BYOD Policy**. If a student witnesses another student interacting with any Social Media account during the school day, they should alert a member of staff.

Parents/carers will be advised that it would be useful if they create their own Social Media account, so that they can monitor their child's activity.

Social Media accounts

When using social media accounts pupils should:

- ***not send personal information***;
- not attempt to open files or follow links from unknown or untrusted origin;
- use appropriate language and;
- only communicate with people they know

Pupils will be expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline.

Social Media posts may be monitored and archived indefinitely.

Pupils should refer to the various **School Internet, ESafety, BYOD and Positive Behaviour Policies** for further clarification.

Social/Collaborative Content

Recognising that collaboration is essential to education, the school may provide limited access to tools that allow communication, collaboration, sharing, and messaging amongst its users such as posting in Google Classroom or commenting or school social media posts.

Pupils are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Pupils ***should be careful not to share personally-identifying information online***.

Mobile Devices Policy

The school will provide pupils with mobile computers and other devices to promote learning both inside and outside of the classroom. Pupils should abide by the same acceptable use policies (**School BYOD, Individual Loan Agreement or ESafety Policy**) when using school devices off the school network as on the school network.

Pupils are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to staff immediately, in particular our **School Technician Mr Emmet Kane**. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices, including use of the school network, may be monitored as in accordance with St. Joseph's Grammar's Internet Policy. The use of Personal mobile phones is permitted in classrooms at the discretion of the subject teacher **but not in public areas** in line with School's **Mobile Phone Policy**.

Personally-Owned Devices

St. Joseph's Grammar School recognise the benefits to learning from offering **all pupils** the opportunity to use personal ICT devices in school to support learners and their learning. The school **BYOD policy** facilitates and supports the use of personal ICT devices i.e. smartphones, tablets, notebooks and laptops in school in furthering individualised student learning.

Any student who wishes to use their own device are expected to use their personal ICT devices in **accordance with the BYOD policy** and must **sign a declaration** agreeing to be bound by the additional school rules and requirements set out in this policy before they will be permitted to use personal ICT devices in school.

Any misuse of personally-owned devices will result in school sanctions as outlined in the **BYOD** Policy.

Security

Students are expected to take reasonable safeguards against the transmission of security threats over the Social Media account(s). This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert the ICT Co-ordinator (**Ms D Dolan)** or Technician **(Mr Emmet Kane)** within school. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads

Students ***should not download or attempt to download or run .exe programs*** over Social Media or onto school resources without express permission from ICT staff. You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

Netiquette

Students should follow the Pupil Online Etiquette (Netiquette) as outlined in their school planner. Below are some netiquette tips relating to Social Media

- Students should always use Social Media, the internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognise that among the valuable content online is unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the internet.
- Students should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. *Once something is online, it's out there- and can sometimes be shared and spread in ways you never intended*.
- Students should be aware that social media and comments posted on personal or school related social media accounts should not impact on the school's business reputation.
  - Where such instances arise school sanctions will be applied as necessary.

Plagiarism

- Students should not plagiarise (or use as their own, without citing the original creator) content, including words or images, from any Social Media account.
- 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 Social Media should be appropriately cited, giving credit to the original author.

Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, ***bring it to the attention of an adult*** (teacher or staff if you're at school; parent if you're using the device at home) immediately.

- Students should never share personal information, including phone number, address, social security number, birthday, or financial information, over the internet without adult permission.
- Students should recognise that communicating over the internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.
- Students should never agree to meet someone they meet online in real life without parental permission.

Cyberbullying

Cyberbullying ***will not be tolerated.*** Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send/favourite/retweet Tweets, media, emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe school sanctions and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained. Police will be contacted as required depending on the nature of the incident.

Pupils should refer to the **Anti-Bullying Policy** for further clarification.

Examples of Acceptable Use

I will:

- Follow good practice (Netiquette) and follow the ESafety advice I have been given when using my own personal social media accounts.
- Use the school Social Media accounts for school-related activities.
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat school Social Media accounts carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies via school Social Media accounts.
- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) on a school Social Media account or another student’s personal social media account
- Use school Social Media accounts at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognise that use of school Social Media accounts are a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school Social Media accounts and uphold the school’s reputation.

This is not intended to be an exhaustive list. Users should use their own good judgment when using social media or commenting on school Social Media accounts.

Examples of Unacceptable Use

I will not:

- Use my own social media accounts or school Social Media accounts in a way that could be personally or physically harmful to me or others.
- Share to, Link to, ‘mention’ or ‘hashtag’ a school Social Media account with inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others – staff, pupils or any organisations or individuals ‘followed’ by a school Social Media account.

- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use a school Social Media account to send spam or chain mail.
- Plagiarise content I find linked to a school Social Media account or other online account.
- Post personally-identifying information, about myself or others on a school Social Media account.
- Agree to meet someone I find online through Social Media in real life.
- Use language on a school Social Media account that would be unacceptable in the classroom.
- Use a school Social Media account for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts, or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

The school will not be responsible for damage or harm to persons, files, data, or hardware. While the school employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. The school will not be responsible, financially or otherwise, for unauthorised transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may result in school sanctions, including:

- Suspension of network, technology, or computer privileges.
- Notification to parents/carers.
- Detention, suspension or exclusion from school and/ or school-related activities.
- Training on safe and acceptable use of ICT.
- Legal action and/or prosecution.

Name: ___________________Signature_______________________ Date: ___________