Cyber-safety Compliance and Conduct Guidelines of St Joseph's College

🚨 Understanding Cybercrime

Cybercrime refers to illegal activities conducted via the internet or digital means. This includes:

- Hacking or unauthorized access
- Phishing scams
- Identity theft
- Cyberbullying or harassment
- Piracy and illegal downloads
- Spreading malware or viruses
- Data breaches
- Financial fraud
- Impersonation or fake profiles

✅ Dos: Safe Practices in the Digital World

1. Protect Your Devices & Accounts

- 🔑 Use **strong, unique passwords** for each account.
- 🔐 Enable **two-factor authentication (2FA)** wherever possible.
- 🔄 Regularly update software, OS, and antivirus programs.
- 📱 Lock your devices with PINs, passwords, or biometrics.

2. Secure Your Online Presence

- 👤 Keep personal info private—avoid oversharing on social media.
- 🔍 Regularly **Google your name** to check what's publicly available.
- 👦🎓 Use your **college email ID only for academic purposes.**
- 🤖 Log out of shared/public systems and avoid saving passwords on them.

3. Be Cautious with Emails & Links

- 📧 Verify the sender before clicking on links or downloading attachments.
- 🚩 Watch for grammar errors or suspicious email addresses.
- 💸 Avoid clicking on "too good to be true" offers or financial promises.

4. Report Suspicious Activities

- 📞 Inform your college's IT department if you receive phishing or scam emails.
- 👦⚖️ Report cyberbullying, impersonation, or fraud to authorities (e.g., National Cyber Crime Reporting Portal: cybercrime.gov.in).

5. Practice Ethical Behavior

- 💻 Use college resources (Wi-Fi, lab systems) responsibly.
- ✖ Avoid downloading pirated software, games, or movies.
- 📝 Cite all sources properly to avoid plagiarism.
- 🚫 Don't try to "test" your hacking skills on others' systems.

6. Educate Yourself & Others

- 📚 Attend cyber awareness workshops or training sessions.
- 🗣️ Share safe online practices with your friends and peers.

✖ Don'ts: Risky or Illegal Online Behaviours

1. Don't Share Confidential Data

- 🚫 Avoid sending sensitive info (bank details, passwords) over public Wi-Fi.
- 📱 Don't share OTPs or PINs—even with friends.

2. Don't Engage in or Support Cyberbullying

- 🤬 Don't send or forward offensive messages, memes, or images.
- 👧⚖️ Harassment (even as a joke) can be a **punishable offense**.

3. Don't Trust Unknown Contacts Online

- 🤖 Be skeptical of random friend requests or messages from strangers.
- 🎣 Don't fall for phishing scams pretending to be friends, professors, or recruiters.

4. Don't Bypass Network Policies

- 🚧 Don't use VPNs or proxies to access restricted college network content.
- 🛠️ Tampering with security settings of college systems is prohibited.

5. Don't Download from Untrusted Sources

- 🕹️ Avoid cracked software, cheat codes, or pirated media.
- □ These often come bundled with malware and spyware.

6. Don't Impersonate or Spread Misinformation

- 👧💻 Fake profiles, fake news, or pretending to be someone else online is **illegal**.
- 💬 Don't share unverified news or screenshots.

📌 Tips for Staying Safe Online (Quick Checklist)

✔ Safe Habits	✖ Unsafe Habits
Use strong passwords	Use "123456" or birthdate
Log out from public systems	Stay logged in on cyber café
Report suspicious activity	Ignore red flags
Verify job offers	Accept random freelance gigs blindly
Respect others online	Troll or cyberbully peers

□ Final Advice for College Students

- Your **digital footprint is permanent**. Think before you post.
- You're part of a wider **digital ecosystem-** your actions affect others.
- Being **cyber smart** is not just about security, it's about responsibility.
- When in doubt, **ask your college's IT support or a trusted faculty member**

Institutional privacy, confidentiality and decorum of the College

In order to protect and maintain the **decorum and the right to privacy and confidentiality** of the College – its teaching-learning time and spaces, premises, processes, possessions, characteristics, etc. –

- Each individual users of mobile phones shall be mindful and respect the **right to privacy and confidentiality** of individuals and of the college.
- Mobile phones are **NOT to be used**, unless explicit permission is obtained, within the college building (Classrooms., Library, Corridors, Exam Halls etc.). Violation of this may lead to the mobile set(s) being confiscated.
- **Making and/or circulating / sending** of Multimedia Medial Services (MMS), reels and TikTok videos, and such other audio-visual contents, in college uniform and of college campus and its activities is **strictly prohibited.**
- Creating and/or circulating of fake and/or unauthorised information is a serious misconduct and a crime punishable by law. Strict disciplinary action shall be initiated against anyone caught or reported recording and/or circulating unauthorised clips, videos, of oneself or others in College Uniform, or of classrooms, corridors, labs or other college premises, or possessions, or processes.

Consequences of Non-Compliance with Cyber-Safety Measures at St. Joseph's College

In the modern era of digital transformation, educational institutions like St. Joseph's College have increasingly integrated technology into every aspect of academic and administrative life. From online classrooms and digital examinations to research databases and internal communications, the reliance on technology has become both a strength and a vulnerability. With this increased dependency on digital tools comes the paramount responsibility of adhering to cyber-safety protocols. Failure to comply with established cyber-safety measures can result in significant consequences, not only for the individual offender but for the wider college community as well. These consequences can range from disciplinary actions under the college's code of conduct to legal implications in cases involving criminal behavior.

1. Disciplinary Action as Per College Policy

a. Violation of Institutional Integrity

When students, faculty, or staff fail to follow cyber-safety guidelines, they not only put themselves at risk but also compromise the institution's integrity. For instance, accessing unauthorized content on college systems or sharing confidential information on public platforms undermines the trust the institution places in its members.

St. Joseph's College, like most reputable academic institutions, has a well-defined code of conduct that includes digital behavior and online ethics. Violations of this code—whether intentional or accidental-can lead to disciplinary inquiries. Disciplinary action may include verbal or written warnings, mandatory counseling, or, in serious cases, suspension from academic activities.

b. Impact on Academic Progress

For students, disciplinary actions can have a direct impact on their academic journey. A student found guilty of engaging in cyberbullying, plagiarism through digital platforms, or unauthorized access to academic resources may face academic penalties. These could include disqualification from certain courses, deduction of marks, or cancellation of examination results. Such actions not only impact the student's current academic standing but can also have long-term consequences on their career opportunities.

c. Deterioration of Personal Reputation

Reputation is a valuable asset in an academic setting. A student or staff member who is reprimanded for cyber misconduct may find their reputation within the college community damaged. In a closely-knit environment like St. Joseph's, word of misconduct travels fast, and individuals may face social alienation, reduced collaboration opportunities, and diminished trust from peers and professors.

Moreover, disciplinary records may be included in academic transcripts or internal files, which could potentially affect applications for scholarships, internships, or higher studies, especially in institutions that emphasize ethical behavior and character.

2. Suspension or Revocation of Digital Privileges

a. Restricted Access to Online Resources

Digital platforms are the lifeline of modern education. Non-compliance with cyber-safety measures can result in the **temporary or permanent suspension of access** to institutional platforms. These may include email services, learning management systems (like Moodle or Blackboard), library portals, cloud storage services, or even the campus Wi-Fi.

For students, this translates into a severe handicap in keeping up with academic responsibilities. They may be unable to submit assignments, take online exams, or communicate with instructors. For faculty members, such restrictions can disrupt teaching responsibilities, student coordination, and research work.

b. Loss of Collaborative Tools

Many educational tasks require teamwork using collaborative digital tools such as Google Workspace, Microsoft Teams, or college-hosted forums. When a member of the college is banned from using these platforms due to cyber misconduct, they are isolated from the collaborative learning process. This affects group assignments, lab work, and project submissions, and can result in group penalties, which also create resentment among peers.

c. Financial Implications

In some cases, students may have paid for premium access to certain academic tools through the institution, or they may be part of funded research projects that rely on institutional digital privileges. The loss of access to these tools can result in financial loss, as students may need to invest in external resources or lose eligibility for project-based funding due to non-compliance.

Furthermore, faculty members involved in funded research or collaborative academic work may lose grants, stipends, or future funding opportunities if digital misconduct is detected and penalized.

3. Legal Action in Case of Serious Cyber Offenses

a. Breach of National Cyber Laws

While internal college policies handle minor offenses, serious violations can invite **legal action under national cybercrime laws**. In India, for instance, the Information Technology Act, 2000, covers a wide range of cybercrimes including hacking, identity theft, cyberstalking, phishing, and the spread of obscene or offensive content. If a student or staff member of St. Joseph's College is found to be in violation of such laws, the matter may be escalated to law enforcement authorities.

Examples of legal breaches include:

- Unauthorized access to or alteration of digital records (hacking).
- Creation or distribution of malware or ransomware.
- Online harassment or cyberbullying.
- Sharing or downloading pirated academic content or software.
- Disseminating hate speech or offensive content through college platforms.

Legal consequences may include **fines**, **imprisonment**, and a **criminal record**. In such cases, the college will be compelled to cooperate with law enforcement and may have no choice but to expel the individual from the institution.

b. Civil Liability

Apart from criminal penalties, individuals may also face **civil liability**. For example, if a student shares another student's personal information online without consent, the affected party may sue for damages. Similarly, if someone's actions result in a data breach that impacts multiple users, victims may collectively pursue compensation through a legal process.

In such scenarios, the college may also suffer reputational harm and face legal scrutiny, which can lead to stricter enforcement of rules and a less trusting environment across campus.

c. Future Employment Implications

A cyber offense that results in legal action can seriously impact an individual's career prospects. Many employers, especially in sectors like IT, education, and finance, conduct background checks before hiring. A record of cybercrime—especially one associated with a reputable institution like St. Joseph's—can result in automatic disqualification from job opportunities.

Even if the offense is not criminal in nature, digital misconduct may still be considered a red flag during recruitment. Employers may perceive the individual as untrustworthy or lacking in professional ethics.

The Broader Impact of Non-Compliance

a. Institutional Trust and Responsibility

Non-compliance doesn't only affect the individual-it impacts the entire college community. One cyber incident, such as a phishing attack that compromises faculty emails or a malware infection from a student device, can disrupt entire systems. It can lead to the shutdown of critical services, loss of data, and compromise of sensitive academic or financial records.

Such incidents often force colleges to divert resources toward cybersecurity measures and investigations, reducing investments in academic infrastructure. This, in turn, affects all students and staff, creating an environment of mistrust and restriction.

b. Ethical Responsibility in the Digital Age

Adhering to cyber-safety measures is not just about avoiding punishment- it's about **being a responsible digital citizen**. St. Joseph's College aims to produce graduates who are not only academically competent but also ethically sound. Digital ethics are now as important as classroom behavior or academic honesty. Non-compliance with cyber-safety protocols indicates a lack of responsibility and awareness-traits that go against the very mission of the college.

Educational institutions function best when all members uphold shared values of respect, accountability, and integrity. Cyber-safety is a shared responsibility, and compliance strengthens the entire academic ecosystem.

Conclusion

In conclusion, the consequences of non-compliance with cyber-safety measures at St. Joseph's College are far-reaching and multifaceted. Disciplinary actions, loss of digital access, and potential legal repercussions serve not only as penalties but also as deterrents to irresponsible digital behavior. As technology becomes even more embedded in education, maintaining a culture of cyber-responsibility is essential.

Students, faculty, and staff must understand that cyber-safety is a shared obligation. Through awareness, vigilance, and adherence to institutional policies, members of the St. Joseph's community can foster a safe, respectful, and productive digital learning environment. The cost of neglecting these responsibilities is too great-both for individuals and for the institution as a whole

01/07/ 2025

Principal
St Joseph's College
Darjeeling