SOUTH POINT SCHOOL

STUDENT OFFICE 365 & EMAIL USAGE POLICY AND CYBER SECURITY

This policy applies to guardians of students and the students themselves, who have been assigned (or given access to) South Point Education Society's licensed Microsoft Office 365 account and an institutional email ID with the domain name @southpoint.edu.in

The Microsoft Office 365 account and its apps including Exchange (the email application) are powerful tools that will help students get a better learning experience. Their accounts must always without fail be monitored by their guardians and should not be left completely on students to handle. In case any guardian has any problem undertaking this responsibility, please inform the school immediately and we will severely restrict the usage rights on the account.

The institutional email ID allotted for each student is to be used for school related purposes only. For students of South Point up to Class VIII, the emails are configured to be used internally within the organisation only and not for sending/receiving emails from outside our domain. Nevertheless, we provide below a list of what constitutes appropriate and inappropriate use of the same:

Inappropriate use of institutional email

Students represent the School whenever their institutional email ID is used. Therefore they must not use the ID to:

1. Sign up for illegal, unreliable, disreputable or suspect websites and services.
2. Send unauthorized marketing content or solicitation emails.
3. Send insulting or discriminatory messages and content.
4. Intentionally spam other people's emails, including their teachers and other students.
5. Conduct personal e-commerce transactions
6. Share their ID with persons external to the School.

The School has the right to monitor and archive institutional email boxes.

Appropriate use of institutional email

Students are allowed to use their institutional email ID for school work-related purposes without limitations. For example, their email can be used to:

1. Communicate with teachers, other students etc. (subject to school policy), related to their work.
2. Log in to official software and applications they have legitimate access to.
3. Provide their email address to other students of South Point and teachers for official purposes.

Cyber security

Email is often a mode of confidentiality breaches, hacker attacks, viruses and other malware. These can compromise the School's reputation, legality and security of our equipment as well as safety of students and staff.

Students and their guardians must:

1. Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
2. Remember passwords instead of writing them down and keep them secret.
3. Change their passwords every two months.
4. Not share your account credentials with any person under any circumstances, including your teachers and other students.
5. Keep the operating system as well as the downloaded applications on their computer as well as mobile devices updated and also install reputed anti-virus applications.
6. Also, they should always be vigilant to identify emails that carry malware or phishing attempts. They should:
    - Avoid opening attachments and clicking on links when content is not adequately explained (e.g. “Watch this video, it’s amazing.”)
    - Be suspicious of clickbait titles or headlines used to psychologically compel readers to crave the information beyond the click.
    - Check properly email ID and names of unknown senders to ensure they are legitimate.
    - Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If you are not sure that an email you receive is safe, please ask the IT Helpdesk of the School. Any breach of security should also be reported forthwith.

Indiscipline

Students and their guardians should take all steps to ensure adherence to the above policy, The following action in particular may attract strict action:

1. Using the institutional email address to send confidential data without authorization.
2. Sending offensive or inappropriate emails to other students, teachers or anyone else.
3. Using institutional email for an illegal activity.

08.11.20