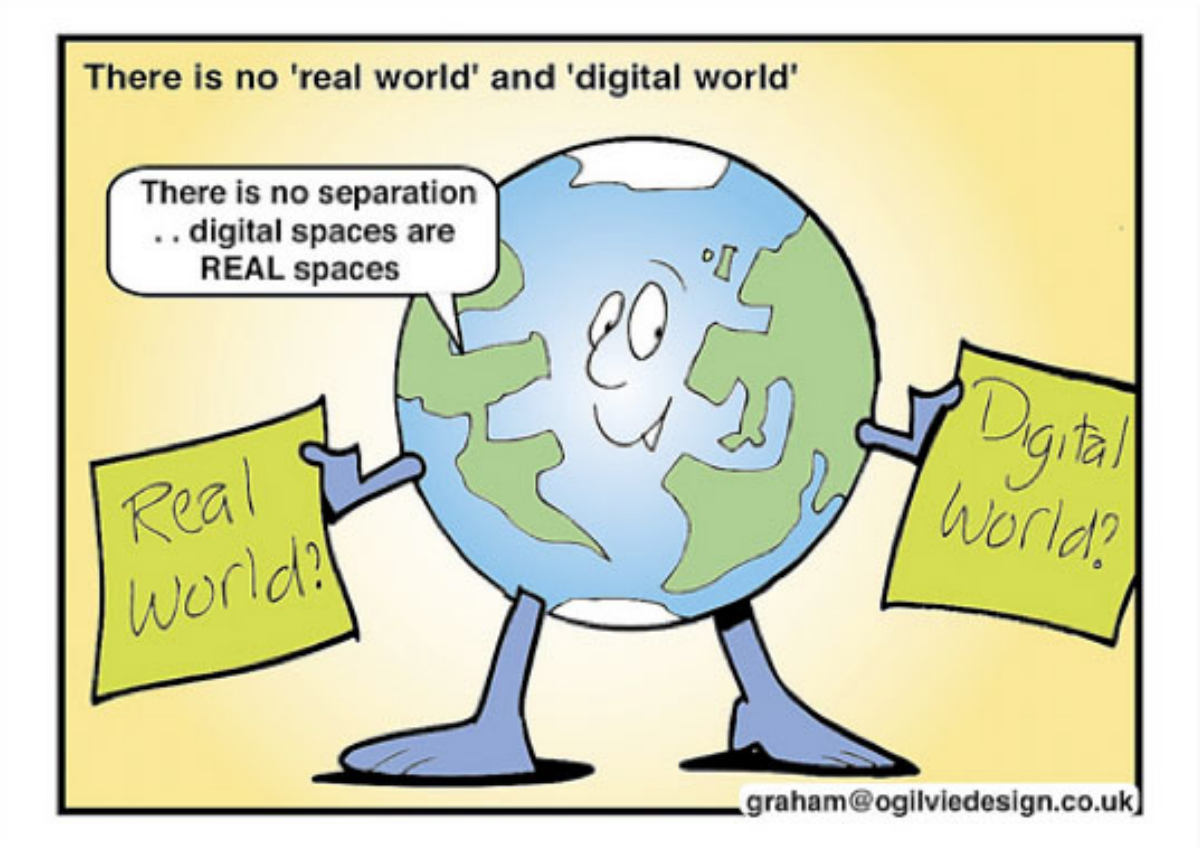
strawberry fields
HIGH SCHOOL

Digital Citizenship Policy
2019



Next Review Date: November 2021

Definition:

At Strawberry Fields High School, digital citizenship is defined as responsible and appropriate behavior while engaging with technology, and the Internet, regularly, in any form or space.

Scope:

The School's Digital Citizenship policy encompasses the impartation of digital literacy and the use of technology in a mindful and constructive manner, with due diligence towards online safety and awareness of norms. Furthermore, it also refers to the response of an individual to membership in any digital community, whether in school or outside school, including the acceptance of, and respect for, multiple perspectives and expressions on online platforms.

Each member of the school community is a responsible digital stakeholder, contributing to a healthy digital environment and, through a planned approach, will be equipped to do so. Members will be made aware of their rights as accountable digital citizens and will be sensitized to the use of digital media with a focus on ethics, etiquette, and culture in a world without cyber borders.

Policy Objectives:

- To develop a dynamic age-appropriate knowledge base related to digital literacy, including but not limited to, enhancing learning with technology, cyber-bullying, cyber-grooming
- To educate all staff and students on digital literacy and age-appropriate use of technology while paying attention to ethics, etiquette, rights and norms
- To disseminate vital and relevant information to staff and students on digital awareness through periodic workshops and regular lesson plans
- To ensure a safe and non-threatening digital environment for staff/students on campus, and provide instruction on avoiding inconsiderate, mean and rude behaviour
- To ensure a safe, non-threatening and efficient computer network for staff/ students on campus
- To provide a secure access to the internet and official school email addresses for all administrative and teaching staff
- To provide secure official school email addresses to high school students for facilitation of scholastic activities
- To ensure that the use of the internet and e-mail is safe and non-threatening for staff/students on and off campus
- To provide age-appropriate access to technology and digital content through various digital subscriptions and customized lesson plans.

Roles and Responsibilities

Administrators

1. To monitor user activity, manage access, and prevent malicious actions on all desktops and servers
2. To ensure that all systems are functional, safe and secure at all times
3. To ensure that maintenance of systems is carried out at regular intervals
4. To ensure that the school network is functional at all times, and to be available for troubleshooting, as and when required
5. To ensure that all software installed on school devices is original and up-to-date
6. To install and periodically update anti-virus software on all school devices
7. To maintain a purchase record for IT-related inventory

8. To maintain a “shared video” folder, the contents of which can be accessed and edited in all classrooms
9. Disable file sharing across desktops in the laboratory
10. Create and maintain official email addresses for all students and faculty
11. Maintain a robust threat management and firewall software, such as, Nebero, which monitors and ensures safe and secure wireless and LAN internet usage
12. To install and maintain CCTV in designated public spaces, classrooms, utility rooms and school buses and allow access to recording to authorized personnel when needed
13. To maintain a digital record of all student and staff - relevant personal and financial information
14. To delete old accounts especially of teachers and students not associated with the school any longer – after a suitably designated time period
15. To liaise with a third-party vendor for maintenance and deployment of the online school portal and mobile application to facilitate electronic fee payment, uploading of circulars, homework, class lists, leave applications and private communication between parents and educators
16. To collaborate with a third-party vendor for the maintenance of the school website
17. To maintain the overhead projectors and smart TVs in collaboration with third party vendors
18. To maintain the hardware evaluation, replacement and maintenance as per functional status
19. Liase with external digital vendors like TeachNext to install, maintain and update software and troubleshoot
20. To reserve the right, without notice, to limit or restrict any computer, network or Internet usage.

Management

1. To strategize and implement a structured approach to spreading digital citizenship awareness amongst all staff, students and parents, including current cyber laws, through periodic workshops and customized IT lesson plans
2. To sensitize parents about their role in ensuring a digitally aware community through sharing of best practices via the school portal
3. To periodically invite industry professionals to address students, faculty and parents on various relevant issues pertaining to digital literacy
4. To approve and permit the use of industry-recognized technology to facilitate curriculum implementation, such as TeachNext, Managebac, Turnitin; and, BridgeU for college applications, and to periodically review the suitability and effectiveness of such technology
5. To encourage and be available for a safe passage for students to report and discuss any kind of online abuse
6. To maintain a confidential Complaints/Suggestion box to enable students to report victimization
7. To ensure that third party vendors who have a contract with school have strong digital security measures in place
8. To display age-appropriate signs saying that bullying is strictly prohibited on our premises and that no such act will go unnoticed or unpunished, as recommended by the Council for the Indian School Certificate
9. For non-IBDP students, to not permit the unauthorized use and possession of digital technology. For IBDP students, to carry and use authorized devices for academic and school-related work only
10. Organize the celebration of ‘Safer Internet Day’ on February 5 every year and the Digital Citizenship Week at the beginning of each new session, which includes multiple interactive activities to strengthen digital literacy
11. Provide access to internet on mobile phone to senior leadership of the School

Educators

1. To role model the responsible use of digital technology through actions within and outside school
2. IT educators to ensure that the students and staff are aware of cyber safety and ethical use of technology through periodic workshops. To disseminate information including, but not limited to, cyber-bullying, cyber-grooming, email spoofing, social engineering, identity theft, job frauds, bank frauds, online gaming, protection of sensitive data, through age-appropriate lesson plans that are delivered during the designated Digital Citizenship Awareness week, which is the first week of the new session
3. To design lesson plans that enable students and teachers to build IT Capabilities that will allow them to facilitate learning and interact critically with information. Furthermore, to follow the model curricula for ICT in Education as delineated by the Department of School Education & Literacy that includes topics on 'Connecting with the world,' 'Connecting with each other,' 'Possibilities in education,' 'Interacting with ICT,' 'Reaching out and bridging divides' and 'Creating with ICT'
4. To commit to the responsible development and inclusion of e-content in their lesson plans to facilitate comprehension levels of students in different subjects
5. IBDP educators to adopt Approaches to Teaching and Learning (ATTL) in their lesson plans and implement it effectively in the classroom situations & to further explore it outside the classrooms through various extracurricular activities
6. To ensure effective usage of subscribed electronic learning resources to deliver lessons
7. To correlate topics that students are studying and their relevance to current times
8. To encourage students to create strong passwords
9. To alert management in case of any student report of online abuse or misuse of technology
10. To check facts and authenticity of information before sharing and forwarding through any digital means
11. Non-IBDP educators to check for unauthorized possession and use of digital technology
12. To be aware of faculty/child's right to privacy and consent when taking photographs for school events
13. To adhere to school norms for maintaining and using their official school email addresses
14. To avoid activities that place unreasonable demand on network capacity or disruption of system operation, including but not limited to, downloading large files without permission from the computer system administrator.

Students

1. To follow the school regulations and norms as detailed in the Academic Dishonesty policy, including but not limited to, cheating, plagiarism, copyright violation, and digital malpractice
2. To attend all scheduled sessions, workshops and lessons related to digital literacy
3. To not access, submit, post, publish, forward, download, scan or display digital materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal
4. To not indulge in illegal Activities, such as using school computers, networks and internet services for any illegal activity
5. To not copy or install software through school's internet without the expressed authorization of the computer system administrator.
6. To not use the school networks and Internet services for non-school related purposes such as private financial gain, commercial, advertising or solicitation purposes, malicious digital use, or for any other personal use
7. To not indulge in misuse of passwords and unauthorized Access of user accounts

8. To understand that they have no right of ownership or expectation of personal privacy to their Internet usage, including personal computers or laptops while on campus, unless authorized
9. To seek authorization to carry and use digital technology for designated purposes only
10. To avoid activities that place unreasonable demand on network capacity or disruption of system operation, including but not limited to, downloading large files without permission from the computer system administrator
11. To not be on or subscribe to social networking sites, because according to the National Cyber Law students below age of 18 are not eligible to have an account on Facebook, Google+ or any other social networking site
12. To understand that creating a false electronic record is an offence under the Information Technology Act and the Indian Penal Code
13. To understand that the school reserves the right to inspect any and all network traffic and files at any time
14. To not use the school's facilities to monitor use of computing or network resources by any other individual, or perform any probing, scanning, "sniffing," or vulnerability testing
15. To not engage in the destruction of the school's digital property and computer laboratories
16. To deposit their hard disks or pen drives with their Grade Tutors and use only when required, under supervision
17. High school students who are authorized to bring phones to submit it to the class teacher before start of the day
18. Authorized students to have access to additional resources such as laptops with specific software to support curriculum access, as issued by the librarian.

Consequences

Students who are found to be intentionally in violation of School's Digital Citizenship Policy will:

1. Have their parents contacted by the school and informed about their actions
2. Have their network privileges revoked
3. In certain circumstances, as directed by the Ministry of Home Affairs, the school will involve the police to deal with intentional serious," illegal" activities.

Parents

1. To read, understand and, when required, acknowledge circulars that are updated regularly on the online school portal
2. To be vigilant about and, when appropriate, act upon, the digital communication from the school through the portal and SMS
3. To help their wards access the technology that the school has subscribed to, such as ManageBac, Turnitin and BridgeU
4. To refer to the following guidelines (that are subject to change) to educate their wards about digital literacy: http://www.safekids.com/child-safety-on-the-information-highway/ https://www.netliteracy.org/safe-connects/safe-connects-psas/

References:

Digital citizenship (part 2): At school and at home. (n.d.). Retrieved from http://blog.core-ed.org/blog/2011/05/digital-citizenship-part-2.html [image]

Independent Schools Association. (2019). Cyber Safety and Security: Guidelines for Schools. New Delhi, India: Ministry of Home Affairs.

Digital Citizenship. (n.d.). Retrieved from https://www.commonsense.org/education/digital-citizenship