St Nicholas School Policies
Online Safety & Safeguarding

Updated: October/2020

St Nicholas School Owner - James Kirsten
St Nicholas Pinheiros Headteacher - Nicholas Thody
St Nicholas Pinheiros DSL - Samantha Waller
St Nicholas Alphaville Headteacher - Laura Bayer
St Nicholas Alphaville DSL - Rosane de Angelo
St Nicholas Brazilian Director - Selma Moura

Introduction

St Nicholas School recognises the vital importance of information and communication technologies (ICT) in today's education. It is a valuable tool and the key to information access, cultural exchange, interactive communication, and global collaboration. It supports meaningful inquiry, promotes authentic learning, and empowers learners with skills that are essential for digital literacy and digital citizenship.

It is essential that our community is aware of protocols for safe, meaningful, and responsible use of technology. This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems.

1. Aims of the policy

- Ensure a safe and secure environment by defining and clarifying the expectations of all members of the school community with regards to safe and responsible use of technology
- Raise awareness about safety and security systems and protocols that the school has in place in order to protect students, parents, and staff
- Outline procedures that will be implemented when responding to the misuse of technology or online safety concerns

2. Responsibilities

At St. Nicholas School, we believe that Online Safeguarding is a shared responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. Therefore the following responsibilities and expectations have been outlined in order to help ensure the safety and security of all school community members while using the internet and devices to communicate, access information, and participate in educational activities.

Leadership

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding practices
- Ensure that policies and procedures are followed by all involved
- Undertake training in offline and online safeguarding
- Liaise with appropriate staff on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of students
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures

All Staff

- Understand that online safety is a core part of safeguarding; as such is everyone's responsibility – never think that someone else will pick it up
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Identify different opportunities to inquire into online safety and make the most of unexpected learning opportunities as they arise (which can have a unique value for students)
- Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites, support them with search skills, critical thinking (e.g. fake news), and signposting, and legal issues such as copyright and data law, including the "Lei Geral de Proteção de Dados" (LGPD)
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff
- Only make contact with children and young people online for professional reasons and in accordance with the policies and professional code of conduct of the school
- Do not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including email, home or mobile telephone numbers; do not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is in immediate risk of harm
- Do not send or accept a friend or follow requests from children or young people on social networks

- Use only school email and account for all school-related activities including Remote Learning and/or any online communication with children and families

Parents

- Help and support the school in promoting Online Safeguarding; discuss Online Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology
- Update software for safe and effective use of programs and applications
- Install security features to allow only age-appropriate content and to prevent malware
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use; do not take or post any photographs or videos of others without their knowledge and permission. This includes school staff, students, and other parents or community members
- Do not share any other school community member's personal information without their permission
- Monitor communications from school and teachers
- Model safe and responsible behaviours in their own use of technology
- Consult with the school if they have any concerns about their children's use of technology
- Help students establish and follow a healthy and balanced routine with regards to attending online lessons, and completing and turning in classwork and homework online
- Encourage the use of technology for positive communication with peers and monitor the use of devices and platforms for this purpose

Learners (Students)

- Know and understand school policies on the use of computers, mobile phones, digital cameras and handheld devices
- Use the internet and devices for constructive, creative and learning purposes
- Access only age-appropriate and reliable materials online
- Take appropriate actions and inform a trusted adult if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they are aware of another student in this type of situation
- Keep passwords safe by not sharing them
- Avoid posting personal information, such as username, complete name, birthday, address and name of the school, online
- Upload images or videos of oneself only when relevant to one's learning and with permission from parents
- Do not take or post any photographs or videos of others without their knowledge and permission
- Always sign out or logout from devices after each use
- Use only positive language when communicating with others

- Understand the importance of reporting abuse, misuse or access to inappropriate materials and are fully aware of the incident-reporting mechanisms that exist within the school
- Always practise academic honesty when producing work by acknowledging information, images and videos produced by others
- Always appear dressed in school-appropriate attire during video conferencing

3. Promoting online safety and positive online behaviour

The internet is an effective tool for multiple educational purposes including communication, collaboration, and research. However, use of the internet, especially in a remote learning situation, can include many risks. Therefore, all school community members must be aware of these risks and educate students about these risks in age appropriate ways as well as monitor their use of the internet for both academic and social purposes.

All media that is shared or posted on the internet may remain public forever and therefore has the potential to cause short term or long-lasting consequences including harm or embarrassment. With this in mind, all members of the school community must carefully select what words and images they choose to post or share on the internet, social media, or communication platforms both internal and external.

It is the responsibility of the whole school community to model appropriate behaviour for students.

Additional safety practices include:

Staff

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation or offend any stakeholder.
- Staff must not post photos related to the school on any internet site including images of students, parents, staff or the school branding (uniform) with the exception of the marketing/medias department, with appropriate authorisations.

Parents

- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.

- Parents need to be aware that the parental control software doesn't replace the need for supervision and education when working on the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.

Students

- Students must not play with or remove any cables etc that are attached to a school computer.
- Students must not post anything on to social networking sites that would offend any other member of staff, student or parent using the school.
- Students must not post anything on any online site that can be constructed to have an adverse impact on the school's reputation.
- Students must not post photos of video related to the school on any internet sites including students, staff, parents or the school branding (uniform).
- Students should be aware that the potential exists for predators to remain entirely anonymous and easily pose as someone else.
- Students should employ a healthy distrust of anyone that they "meet" online unless their identity can be verified. Do not arrange to meet anyone you have met on the internet - people are not always who they say they are.
- The use of chat rooms and social networking sites are not permitted in school.

4. Information and network security guidelines

St. Nicholas School uses state-of-the-art technology from globally recognized companies and is in line with good market practices in the technology industry. St Nicholas' own internal infrastructure model was a reference at a technology conference at Dell's headquarters in Santa Monica / California in 2016 for being the only elementary school among universities and colleges in Latin America.

Our IT team is made up of technicians and specialists with undergraduate and graduate degrees in the field. All have internationally recognized certificates and training in their area of expertise by our partner companies: Microsoft, Google, Dell and Apple.

Hardware

Our entire technology park is made up of Dell and Cisco equipment. Servers have the updated Microsoft operating system, with original licenses and Kaspersky antivirus. The school's data is encrypted and stored in a secure and restricted location. All computers at the school use the latest version of the Microsoft operating system and users do not have administrator access, except for the IT staff. Learners most frequently use Chromebooks which are virus free and where nothing is stored locally. The entire system is online and manageable through Google Suite for Schools.

Network

Each user is registered in the network system by an id and password (Active Directory) that is for personal use, non-transferable and of exclusive knowledge. With this password, each user has the necessary rights to use the network, internet and hardware devices (computers, notebooks, tablets, etc.). We use a different profile among administrative staff, teachers and students according to their age group and types of permissions. The school's entire network infrastructure is protected by encryption, protocols and security policies. No external device has access to the school's internal network, even if connected via our wifi.

Internet

We use the SonicWall / Dell professional, world-renowned firewall where the entire internet browsing filter is made, blocking it through a worldwide blacklist in cooperation between major technology companies and is fed daily with millions of contents, keywords and web addresses. These sites with inappropriate access can be tracked by users.

We have a SonicWall certified team and we also count on a SonicWall partner company for any help that is necessary, being able to generate reports of accessed sites, blocked sites and types of content per user.

All students and teachers can use the school’s wifi network to access the internet from their own devices, however it is necessary to use the network id and password described above. This access, through our wifi is also trackable, even when using personal devices.
The wifi network for personal devices is separate from the main school network and is completely isolated, with no access to servers, machines and other internal equipment.

Google Technology

The school uses Google technology (G Suite for Schools / Gmail) to create our mailboxes, where all the security, encryption and reliability of the tool is managed by Google. We have support from Google when necessary. Any material that violates international laws, copyright and / or inappropriate content, is constantly monitored through Google's artificial intelligence and subject to notification by national and international authorities.

Teachers and students use the Google Drive and Google Classroom tools for assignments and homework. These tools go through a strict security control adopted by Google itself.

St. Nicholas emails are exclusive for professional use and, like any professional tool, can be and will be monitored as necessary.

Use of digital and video images

Many educational activities involve and can be enhanced by recording images for assessment or evidence of activity. Such images are managed and stored confidentially and securely.

Images to be used internally within the school

Staff may take digital / video images to support educational aims but must follow this policy concerning the sharing, storing and publication of those images.

The purpose of the photo must be for pedagogical purposes only.

Portrait images can be used if appropriate and if for sharing only with the child (ie name tags) or with the family of the child.

Images of groups should focus on the activity rather than the individual and if the image is destined for one parent

Care should be taken when taking digital / video images to ensure that students are appropriately dressed and are not participating in activities that might bring risk to the subject or the group.

It is the responsibility of the photographer to be aware of the risks associated with taking, storing and sharing images.

Storage of photos taken to be used internally within the school

Photos must be taken off/deleted from devices and be stored in the appointed shared Google Drive Folder the same day. Each teacher has access to his/her classroom folder; heads of department have access to the groups under their care, and heads of school have access to the whole folder. The marketing/media department will process and store these images in the digital archive for future use.

The photos can only be shared using the guidelines below. Once the photos have been shared on the destination platform they must be deleted from other locations.

Photos stored on the drive should not be identifiable by the student's full name or other identifying tabs other than the first name.

Sharing of internal photos

- Photos can be shared informally on the device with colleagues within the year group and for pedagogical purposes or safeguarding purposes.
- Photos can be shared by the section or school leadership for pedagogical or safeguarding purposes .

Photos cannot be shared informally on the device with any other adult than stated above either inside or outside the school.

Images to be used internally within the school can only be shared by being uploaded to passworded pedagogical sites used by the school for educational purposes. The only people with access to the sites will be people in possession of the password. Improper unauthorized access to passworded sites is subject to disciplinary procedures.

Images to be used externally from school

All photos with an external destination require specific permission from parents

- Photographs published on the website, social media, or elsewhere that include students will be selected carefully and will comply with this policy.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Student Digital Safety in sharing images

- Staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Students must not take, use, share, publish or distribute images of others without their permission.

When searching for images, video or sound clips, students will be taught about copyright and acknowledgment of ownership.

5. Student use of personal devices

Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a staff member. The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones. Devices should be turned off or switched to silent mode in order to avoid

disruptions. Mobile phones and personal devices use are not permitted in certain areas within the school site such as changing rooms and toilets.

Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to instead contact the school office if they need to communicate with their child.

Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences. It is the joint responsibility of parents/guardians and the school staff to establish expectations and educate students about appropriate use of personal devices.

Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or guardians.

6. Responding to incidents of misuse

It is the responsibility of all members of the school community as responsible users of ICT to understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible, or very rarely, through deliberate misuse. Listed below are the procedures that will take place in response to any apparent or actual incidents of misuse**:**

Plagiarism

Staff and students should not plagiarise work that they find on the internet or anywhere else. If you wish to use someone else's work, make sure you quote and give credit to the authors.

Everyone should respect copyright. If unsure, students or staff should request permission from the copyright owner. This includes the copying of music files and CDs.

Cyberbullying

By cyberbullying, the School is referring to: bullying by email, messages, images, calls or other electronic communication. It includes:

- Use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites (including social networking sites)
- Hijacking or hacking email accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms or on instant messaging services
- The use of Social Media for the use of bullying, grooming, abuse and radicalisation.

Communication

Communication between adults and between children/young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries.

All communication between staff, students, and other school community members must be conducted in a professional manner no matter the device or platform being used. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, webcams, websites, forums, and blogs.

Illegal activity

If any apparent or actual misuse appears to involve illegal activity e.g.

- Child sexual abuse images
- Adult material which potentially breaches the articles 233 and 234 from the Brazilian Código Penal.
- Criminally racist material
- Other criminal conduct, activity or materials

The Heads of section and Safeguarding Team are informed immediately. The Safeguarding Team will then determine further steps that need to be taken.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that appropriate steps are taken to investigate, preserve evidence and protect those involved according to the Safeguarding Policy.

It is important that any incidents are dealt with as soon as possible in an appropriate manner, and that the relevant members of the school community are kept informed. Incidents should be reported to the heads of site, and will be taken to the leadership team. Incidents of misuse will be subject to behaviour/disciplinary procedures.