Solid Foundations Primary School

Technology Policy (2023/11)

For the purposes of this policy, cell phones, tablets, IPADS, notebooks, laptops and any other technological device that operates on electricity or battery power with or without internet access is called a "device" (with the exception of calculators and digital watches).

a. Student use of devices:

1. Devices must be handed in at the school office before school begins. They are stored in the principal's office for safekeeping.

2. The school does not accept any responsibility for the loss, theft or damage of devices handed in.

3. Pupils may collect devices from the office at the end of the day. No pupil may collect a device on behalf of another pupil.

4. Devices may not be used in class for projects unless the teacher has given permission for a child to do so.

5. Should a pupil fail to comply with the abovementioned stipulations and a device is seen on their person or in their suitcase during the course of a school day, the school is entitled to request that the device be surrendered to the school for a period of at least a week (first offence). If the child is subject to a second offence, the device will be surrendered to the school for a month. Failure to comply with points 1 – 4 above will also result in a demerit being issued.

6. The school may conduct spot checks in suitcases or kit bags or on the child's person to ensure the above.

7. No devices are permitted in After Care, after school hours, or during the school holidays, unless purposefully given to the pupils by a supervising teacher.

8. Currently, e-readers are the only exception to the above and may be brought onto the school premises for the express purpose of reading. If the e-reader is used for any purpose except for reading, the repercussions mentioned in point 5 apply.

9. Under no circumstances may a parent use any device for photographing or videoing of a person other than their own child on the school premises, or during entrance examinations and tests.

b. Student use of Chrome books:

1. The school permits the use of school-owned Chromebooks as an educational resource.

2. Chromebooks are the sole property of the school and may only be used in class under teacher supervision.

3. The school will maintain annual Securely Software licensing to ensure the safety of our pupils while browsing.

4. Chromebooks are regarded as educational tools and may not be used for any personal purposes other than school-related assignments or tasks.

5. Grade 5 – 7 students must complete a mandatory Chromebook usage lesson at the beginning of each year (in the first lesson that they are used).

6. New teachers must attend a short Chromebook training lesson. Arrangements can be made with the Deputy Head in this regard.

7. Chromebooks must be scheduled for use ahead of time (booked on Google Drive).

8. Chromebooks are carried to classrooms in Chromebook bags, and returned to the storeroom/locked cabinet in Mr Swiegers' class or Mrs van Dijk's class after they have been used. Mrs van Dijk and Mr Swiegers must ensure Chromebooks are locked away at the end of each day.

9. The transportation of Chromebooks from class to class must be fully supervised at all times.

10. Teachers must ensure that students handle Chromebooks with care (i.e. not allow students to eat or drink near Chromebooks) and shut Chromebooks down after they have been used.

11. Pupils may not delete their browsing history.

12. Pupils may request to use Chromebooks and have access to the internet for school projects, before, during or after school (in After Care homework classes), as long as they always do so under the supervision of a teacher and ask Mr Swiegers for access. Non-permanent After Care pupils (Grade 4-7 only) may have access to Chromebooks and the internet, for school work only, during After Care homework classes at no cost. It is compulsory that this is pre-

arranged with the school (24 hours in advance). However, this does not entitle the user to After Care lunch or to free After Care supervision once the homework class is finished. The user will need to be fetched immediately after homework class or he/she will be charged an After Care fee for the afternoon.

c. Homework and printing:

1. Homework in the senior grades (4 – 7) may be typed if the subject teacher has granted permission for pupils to do so.

2. The school will print out projects or pictures for pupils at a cost of R5 per coloured A4 page and R2 per black-and-white page. Printing is done by emailing the work to the school (admin@solidfoundationsprimary.com) or Mr Swiegers (jswiegers@solidfoundationsprimary.com).

3. Staff may not download copywrite-protected content for school use, unless fully referencing the source.

4. Staff may not print or photostat any pages not directly related to teaching unless special permission has been obtained to do so from the principal.

d. Staff computer:

1. The administrative and teaching staff are permitted to use two communal computers on the school premises (hall and media centre).

2. Printing from the computer for teaching-related purposes is permitted.

3. Content downloaded or saved onto this computer will not be regarded as permanent. Staff are to keep files and important personal information on flash drives or backed up on the cloud or their own private computers. The school may delete files and content from the staff computers at any time.

e. Staff cell phones:

1. Staff may not talk on their cell phones or text for casual purposes during teaching hours. This applies to all grades and all subjects (music, art and PT included). Cell phones may be used at break and before or after school by staff members not on playground duty.

2. Staff are requested to be a part of the Solid Foundations formal WhatsApp group. Consent must be given by each staff member who is on this group, or any other WhatsApp groups created for staff communication purposes.

3. The Solid Foundations formal WhatsApp group has been created to send relevant school-related messages. It is the responsibility of the individual staff member to check their phones daily and during breaks for any messages. No casual messaging or non-school pertinent messages may be sent on this group. Casual staff discussions are held on the “Share and Care” WhatsApp group. Participation in this group is voluntary.

4. Staff may post personal announcements on the formal staff WhatsApp group, e.g. “I got engaged”, but responses to the announcement must be sent to the staff member’s private Whatsapp number and not posted on the formal group.

5. The formal WhatsApp group cannot be seen as the most reliable platform to relay messages that need a “same-day” or “instant” reply in an urgent response time. Urgent messaging (response required in less than 24 hours) will also need to be communicated directly to staff if the acknowledgement from the staff member on the WhatsApp group is delayed. Staff are requested to view the formal group WhatsApp messages at least once daily during school terms.

6. Staff are requested to refrain from messaging on any WhatsApp groups after 9 o’clock at night or before 9 o’clock on weekend or holiday mornings.

7. Staff are invited to photograph fun events or appealing lessons on their cell phones. Photos can be sent to the Deputy Principal, either via WhatsApp or preferably via email, who will upload images onto the school website.

f. YouTube and videos:

1. Staff are strongly encouraged to use clippings and videos for educational purposes. All clippings and videos must be “all ages” and relevant to the syllabus at hand.

2. Pertinent clippings with age restrictions need to be cleared by the principal before viewing in class.

g. Projectors and whiteboards:

1. All classes are all equipped with projectors and whiteboards. Each class also has a set of speakers or a soundbar.

2. Staff must notify the principal immediately if any of these devices are not in full working order.

3. Teachers using the hall projector are requested to leave the remote control accessible in the hall cupboard. It is each teacher's responsibility to turn off the projector at the conclusion of a lesson.

h. Social Media

1. Pupils, parents and employees may not use social media (including emails, Facebook, X, TikTok, WhatsApp etc.) in any way that may be seen as insulting, disruptive or offensive by other persons, or harmful to the morale of the school.

2. Examples of forbidden transmissions include sexually-explicit messages, sexually-themed cartoons or jokes, unwelcome propositions or love letters, ethnic or racial slurs, or any other message that can be construed to be harassment or disparagement of others based on, inter alia, their sex, race, sexual orientation, age, national origin, religious or political beliefs.

3. Staff may not create WhatsApp groups with their parents. Broadcast groups are, however, permitted.

4. Parents give their permission in the basic school contract for their children's photographs to be used on social media platforms, which is publicly accessible. Parents not wanting their child's photograph to be taken or publicly viewed must make a request in writing to the school.

i. Further Privacy and POPIA compliance

All personal information is considered confidential and will only be shared with teaching and administrative staff and data subjects (on request).

1. Access to Wi-Fi

1.1. The school provides Wi-Fi access for all staff members.

1.2. The Wi-Fi may be accessed via a password that is available from the principal.

1.3. The Wi-Fi password may be changed from time to time and these changes will be communicated to the staff.

1.4. Access to the school Wi-Fi is conditional on appropriate use.

1.5. Whoever accesses the school Wi-Fi may not:

1.5.1. Use the Wi-Fi to conduct illegal activity.

1.5.2. Use the Wi-Fi to access peer to peer downloading.

1.5.3. Use the Wi-Fi to access content for personal (not school related) entertainment.

1.5.4. Use the Wi-Fi to share personal information with outside parties.

1.5.5. Access inappropriate or explicit content.

2. Password management

2.1. The school requires all electronic personal information files to be secure and accessible via authentication.

2.2. One of these steps is a mandatory random password that contains at least eleven characters.

3. Secure destruction and disposal of computer data

3.1. All computer data is deleted from hardware and cloud storage once the retention period for that data is passed.

3.2. Data relating to personal information may only be stored on the cloud and is password protected.

Device requirements

4.1. Teachers who use personal devices to access personal information of students, parents/guardians, or other staff members must ensure that their devices are secure.

4.2. Devices must require a password to access and may not be left accessible and unattended.

4.3. Devices must be protected by a firewall and anti-virus software.

5. Travel risks and working from home

5.1. No personal information may be shared or discussed in a public venue.

5.3. When working from home, staff must ensure that all necessary precautions are taken regarding the safety of personal information.

6. Monitoring and compliance

6.1. The School Information Officer is responsible for the safe management of data in the school and may do periodic checks to ensure that stakeholders are complying with the above-mentioned guidelines.