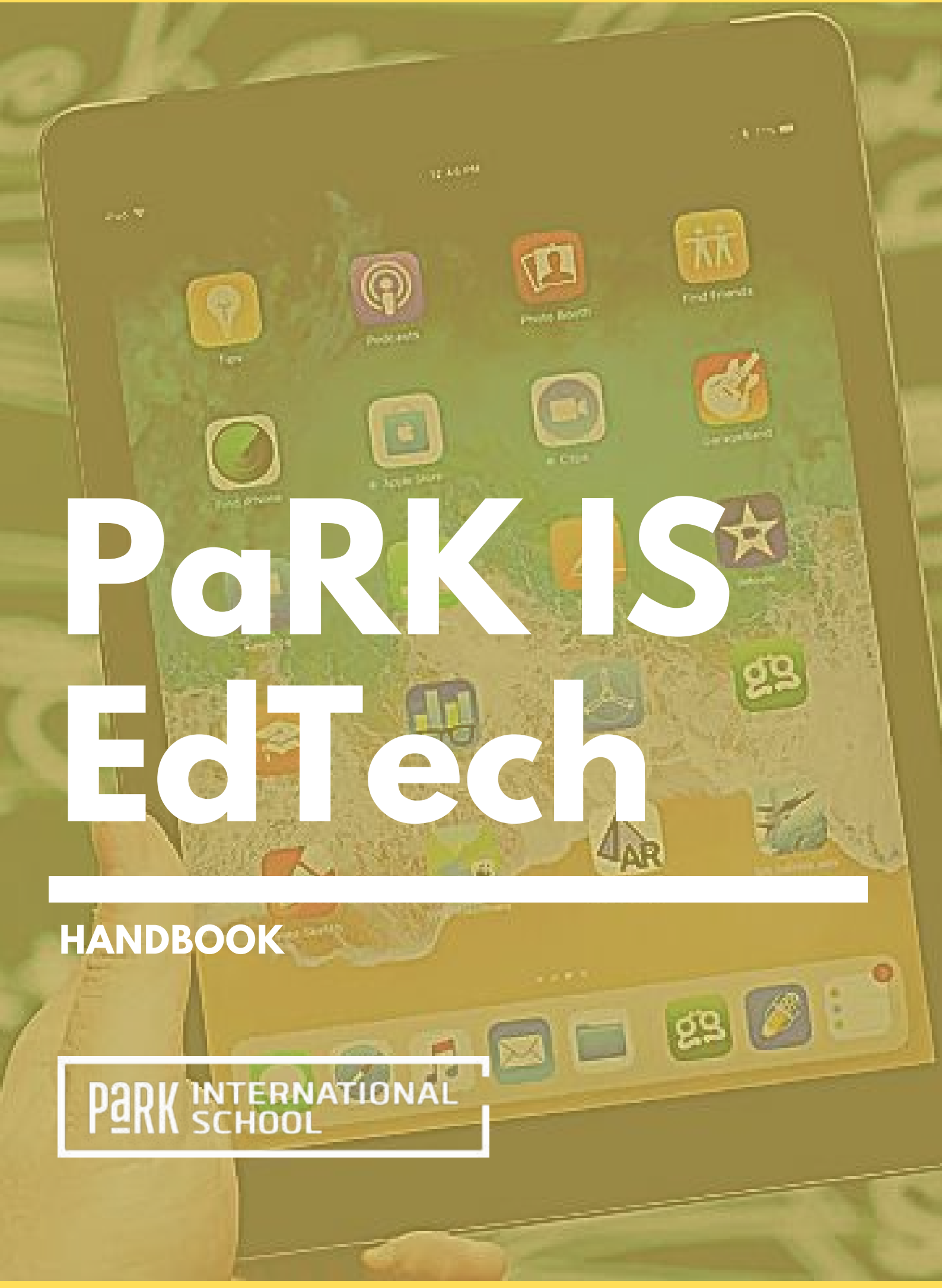


# PaRK IS EdTech

## HANDBOOK

PaRK INTERNATIONAL SCHOOL

## Table of Contents | EdTech PaRK IS

## 1. Introduction

The use and integration of technology is part of PaRK IS's core mission, aligned with preparing students for their future life and challenges.

**Purpose of the EdTech Team**:

Bringing people with pedagogical and technical skills together to support the teachers.

*Empathy and understanding for teachers play a critical role in the effectiveness of ed-tech teams and, similar to how teachers must nurture every student in their classroom, so must EdTech teams encourage even the least technology-inclined among us.*

### 1.1. Foundations of management

- Device management
  - 1 to 1
  - Shared
  - 1 to all
- Classroom management
  - LMS (iTunes U; Google Classroom)
  - MDM (Jamf; Apple Classroom)
- Content management
  - Personal and instructional training (Edtech MeetUps)
  - Publications (iBooks, iTunes U)

***Using technology without adapting teaching methodology brings no change.***

### 1.2. Devices

| | Students | Devices |
|---|---|---|
| **Lower Junior School** | School iPads shared 1:4 | iPad |
| **Upper Junior School** | BYOD iPad 1:1 | iPad |
| **Lower Senior School** | BYOD iPad 1:1<br>Grade 8 - transition year iPad to a laptop<br>RYOD iPad 1:1 (Grade 8 new students only)* | Laptop + iPad |
| **Senior School** | BYOD Laptop<br>The basic requirements for the laptop we advise students to have at PaRK IS are:<br>○ Processor: i5 or higher;<br>○ 8GB RAM<br>○ 256GB SSD<br>○ NVIDIA/RADEON graphic card<br>○ 11+ inch screen | Laptop |

* For new students that start Grade 8, PaRK IS has a Rent Your Own Device (RYOD) system for families that don't wish to buy equipment. Refer to Appendix 4 to see the RYOD Agreement.

**BYOD iPad 1:1**

The iPad we advise students to have at PaRK IS is the iPad 32GB 8th Generation. They can use a different model as long as it's a version equal or superior to the iPad 6th Generation (2018).

Bundles available to be acquired by PaRK IS:

| Opções | Descrição | Pronto Pagamento | 3 Prestações (Set, Out, Nov) |
|---|---|---|---|
| Bundle #1 | • iPad 10.2" Wi-Fi 32GB - Space Grey<br>• UAG Capa Metropolis iPad 10.2 Cobalto | €442 | €147.34 |
| Bundle #2 | • iPad 10.2" Wi-Fi 128GB - Silver<br>• UAG Capa Metropolis iPad 10.2 Cobalto | €541 | €180.34 |
| Bundle #2 | • iPad 10.2" Wi-Fi 32GB - Space Grey<br>• Película Laut Prime Glass iPad 10.2 2019<br>• Pipetto Origami N02 Pencil Shield iPad 10.2 2019 Royal Blue | €490 | €163.34 |
| Bundle #2 | • iPad 10.2" Wi-Fi 128GB - Silver<br>• Película Laut Prime Glass iPad 10.2 2019<br>• Pipetto Origami N02 Pencil Shield iPad 10.2 2019 Royal Blue | €589 | €196.34 |

### 1.2.1. Delivery & Return Procedures

The iPad is considered a working tool, both for students and staff and, as such, each one is responsible for the device and to know how to operate it. The EdTech Team provides courses for staff at the beginning of each year, depending on the level of proficiency. This way, all staff is an active agent in helping students manage their devices and work with it to its full potential.

**Students**

**Delivery** - all iPads acquired through the school are delivered to the student in the beginning of the school year, along with access to an individual @park-is.com email account. The student is responsible for creating his Apple ID.

**Return** - iPads remain with the student and don't need to be returned, unless the iPad is from the RYOD programme. In that case, the student needs to return it by the end of the school year to the school's operational assistant or in the MakerSpace (Alfragide). The iPad must be returned with all items initially delivered and this form filled in.

**Staff**

**Delivery** - an iPad is provided by the school to all staff teaching from Grade ELS - 8 in the beginning of the school year, along with access to an individual @park-is.com email account. The staff is responsible for creating their own Apple ID.

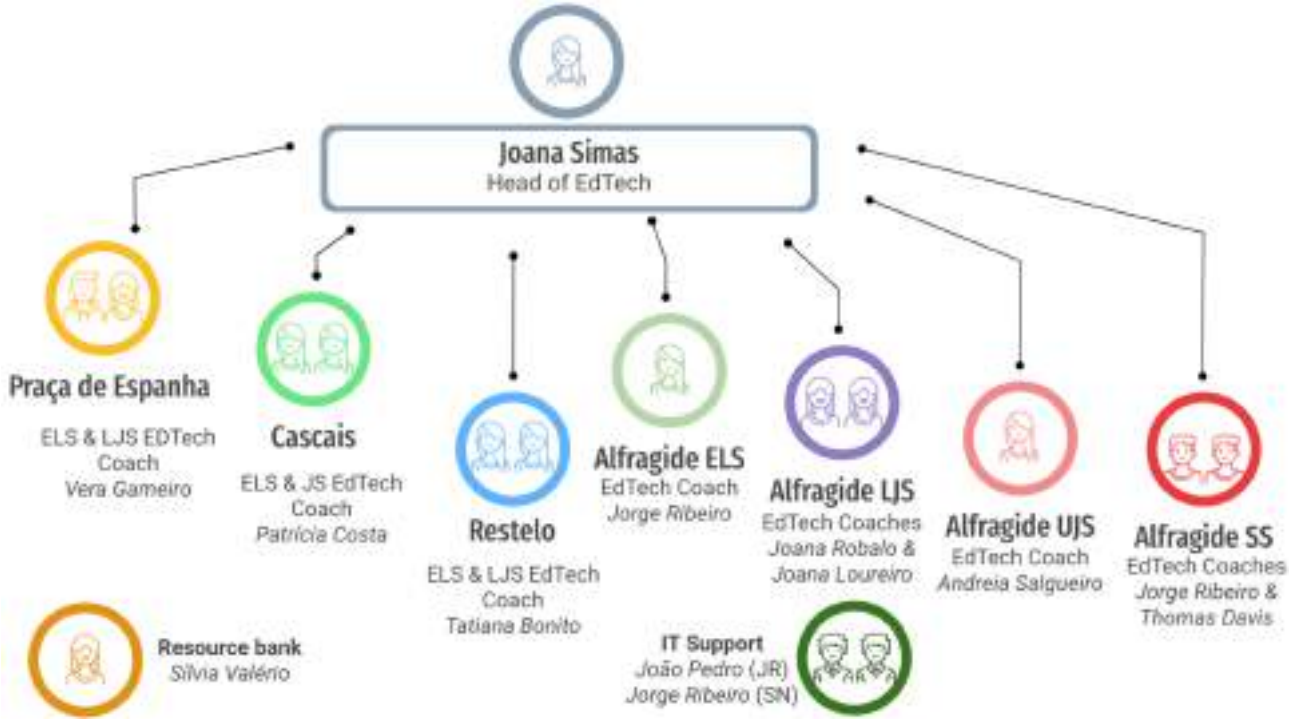
**Return** - iPads are returned at the end of the school year for maintenance and reconfiguration purposes. Staff need to return it to an EdTech member of their campus or in the MakerSpace (Alfragide). The iPad must be returned with all items that were received at the beginning of the school year and this form filled in - available with a member of the EdTech Team or in the MakerSpace.

## 2. Organization by campuses and Team

The EdTech team is organized by EdTech Coaches present in all campuses, supervised by the Head of EdTech.

Our resource bank serves as a depository for materials created for the whole school.

Teachers will be assisted according to a defined schedule and according to their level of technological proficiency. A Follow Up is maintained throughout the year, with different moments of recommendations for professional development and linked to the teacher's PDP.



**Technology proficiency levels:**

| | Use of the iPad \| Laptop | Use of Google Apps \| Microsoft 365 | Use of other apps / digital resources | Integration in curriculum | Content development |
|---|---|---|---|---|---|
| Rookie | Needs assistance and guidance through the iPad or laptop main features. | Needs assistance and guidance through the use of the main Google Apps | Starts to try out the use of an app suggestion in a specific class. | Occasionally uses a digital resource or app for a specific task in class. | Creates simple content, such as documents and presentations, using only one or two types of digital support tools. |
| Beginner | Is able to navigate through the iPad or laptop main features | Uses some Google Apps to share work with students. | Follows app recommendations and uses some of them in classes. | Uses digital resources in some classes, as a starting or ending point. | Creates instructional content being able to use two or three different types of digital support tools. |
| Expert | Able to use new iPad features and laptop extensions or add-ons and explore others suggested. | Uses the main Google Apps as a way of sharing resources and tasks with students, including some collaborative tasks. | Follows app recommendations and uses them in classes, also searching for other suggestions. | Develops a learning unit with specific apps as enablers of success criteria. | Creates a range of instructional content, using more than three types of digital support tools |
| Jedi | Independently explores new iPad features available through updates or laptop tools, extensions or add-ons. | Uses the main Google Apps as the baseline of collaborative work developed with students. | Searches, suggests and evaluates different apps and digital tools according to their pertinence in classroom use and curriculum objectives. | Develops projects and learning units alongside the curriculum, by using a range of diversified digital tools, all contributing to meet the success criteria of the curriculum. | Creates a full range of diversified and origina instructional content, using several different digital support tools and according to the curriculum. |

Teachers reaching a high level of professional proficiency in the use of technology in the classroom may be eligible as EdTech coaches.

**Note**: All of the EdTech Coaches must have Google Certified Educator (GCE) Level 1 and 2.

### 2.1. Roles/Expectations

#### 2.1.1. *Head of EdTech*

- Professional development and training for teachers through the EdTech meetups and internal workshops, in the beginning, middle and end of the school year, as well as whenever the need arises to focus on specific apps and platforms.
- Software, hardware and online resources support for students, parents and teachers on everything iOS related, including deployment and enrolment of devices in the iPad 1 to 1 school program, technical support, troubleshooting and maintenance.
- Technology integration into lesson plans through educational projects, iTunes U courses/"sebentas" and iBook publications, in alignment with the coordinators and heads of all departments and sections.
- Digital citizenship, internet safety and implementation of the usage procedures for students and teachers.
- Instructional strategies, digital tools and platforms, best practices and feedback, Jamf, iTunes Connect and iTunes Site Manager.
- Start implementing eTwinning on our campuses.
- Reflect and present the overview of the school year to all Heads and Headquarters - HERE (2020)

#### 2.1.2. *EdTech Coach*

- Help educators integrate technology into their classrooms and their curriculum providing support in pre-established meetings (ELS/ 1st and 2nd grades one time per period, 3rd and 4th biweekly).
- Organize the EdTech biweekly meetups with the EdTech team.
- Prepare workshops answering teachers' needs.
- Create support materials (courses).
- Share with all the school teachers apps, articles and learning opportunities (such as conferences and webinars)
- Search external opportunities to share our best EdTech practices and projects.
- Available by email to answer teachers' questions.
- Available to meet with teachers and to help them during classes.
- Coach the teachers of their section.
- Start implementing eTwinning on our campus (Alfragide).

## 3. EdTech MeetUps

EdTech MeetUps will be held twice every term as a sharing time for new app / digital tools developments and best practices. HERE you can find the sessions calendar.

Teachers are welcome to share and present to an audience in different moments as well (for example, sharing practices during VS after this info was collected HERE).

Tech Sessions were created as a moment for sharing good practices between teachers, having guest teachers present different ways they have integrated technology or app features that are important to be shared. Below you can find the agenda and a resume of last year's sessions:

| | | |
|---|---|---|
| **PaRK IS Tech Sessions Season 1** | Agenda | Video |
| **PaRK IS Tech Sessions Season 2** | Agenda | Video |

## 4. Teacher Training and Follow Up

Depending on their level, teachers must complete the suggested training as part of their professional development plan. Throughout the year, the EdTech team will suggest other training based on the offer available. HERE you can find a general survival kit for all campuses, with videos and instructions of our main platforms.

| | Teachers applicable | Campuses | Requirements | | Due date |
|---|---|---|---|---|---|
| | | | Training | Follow Up | |
| **Level Rookie** | New teachers | All campuses | Initial GSuite Training & iPad Training | Assessment & follow up by EdTech Team | Midterm |
| **Level Beginner** | PaRK IS teachers for 1 -2 years | JS + SS | Training before Google Certified Educator Level 1 (offered by the school ) | Assessment & follow up by EdTech Team | By the end of the school year |
| **Level Expert** | PaRK IS teachers for 3 - 4 | JS + SS | Google Certified Educator Level 1 & Microsoft Certified Educator | Assessment & follow up by EdTech Team | |
| **Level Jedi** | PaRK IS teachers for 5 and beyond | JS + SS | Google Certified Educator Level 1 & Level 2* & Microsoft Innovative Educator Expert | Assessment & follow up by EdTech Team | By the end of the school year |

*Level 2 recommended - not supported by the school

Teachers will be followed and assisted by the Edtech team coaches according to their proficiency level and needs.

| | Assistance in classes | Follow-up |
|---|---|---|
| **Level Rookie** | Once per week / Whenever necessary | Feedback meeting in the same week |
| **Level Beginner** | Twice per term | Feedback meeting at the end of each term |
| **Level Expert** | Once per term | Feedback meeting at the end of each term |
| **Level Jedi** | Whenever pertinent | Feedback meeting when relevant |

### 4.1. (Virtual) conferences with EdTech Team

The EdTech Team works in collaboration with an external consulting firm to support teachers.

We have a regularly scheduled series of (online) sessions led by our EdTech Team. They present on specific topics and allow time for questions and discussion at the end to address specific teacher needs and interests.

Our **leadership series** is designed to support strategy and planning. These planning sessions explore technology's role in learning by highlighting real school stories, describing key elements for leaders planning initiatives, and providing ideas for integrating and measuring the impact of technology in the classroom.

**Coaching by EdTech Team**

Our EdTech Team is available to work with you and all departments virtually and onsite (when restrictions lift) on scheduled days throughout the year. The team offers the customized support, working side by side with the teachers and students to meet individual needs and goals for learning and teaching with technology.

### 4.2. PaRK Professional Learning Plan - September - August (with Joy of Professional Learning)

One to Many - 1 hour workshop

One to few - 1 x 30 min leadership planning

One to One - 1 x 30 min coaching session

* 1 extra hour per session is earned with full team participation

## 5. MakerSpace

The MakerSpace (Alfragide, Room 2.16) is available through previous scheduling, which you can book HERE.

Teachers can book the space in advance for a 30 minutes tryout of the materials / technology available or for 1 hour with their classes. A member of the EdTech Team is always available to give assistance.

HERE is a brief overview of the materials available.

For other campuses, a **MakerKit** will be provided to allow them to create a small space to create / use technological tools. The MakerKit will contain:

- Two green cardboards
- iPad stand or tripod
- Other materials available through the previous request

### 5.1. PaRK IS base Apps and Digital tools

Our main work is developed in Google Apps for Education, using others as complements or with a pedagogical purpose.

Recommended apps and programs are based on students' levels and type of work.

| MAIN APPS | Classroom-based work | Subject resources | Video conference |
|---|---|---|---|
| **Early Learning School** | Seesaw | - | Zoom |
| **Lower Junior School** | Google Classroom | Workbooks<br>Google Classroom / Drive | Zoom |
| **Upper Junior School** | Google Classroom | PaRK IS Workbooks | Zoom |
| **Lower Senior School** | Google Classroom | To be determined by each department. | Google Meet |

| | | | |
|---|---|---|---|
| **Senior School** | Google for Education Apps \| Microsoft 365 | | Google Meet |

**Recommended Devices**:

| | |
|---|---|
| iPad (in progress) | Laptop Windows |

## 6. E-Safety Policy

### 6.1. Introduction

The school aims to ensure that every student in its care is safe, and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose more significant and more subtle risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs
- Social networking sites
- Chat rooms
- Music/video downloads
- Gaming sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as smartphones and tablets

This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

While exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.
We understand the responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents include students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Agreements cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smartphones, etc.).

### 6.2. Roles & Responsibilities

#### 6.2.1. *(Executive) Head and the Senior Leadership Team*

The (Executive) Head of School is responsible for the safety of the members of the school community, and this includes responsibility for e-safety. The (Executive) Head of School has delegated day-to-day responsibility to the Head of EdTech and the Well-being department. In particular, the role of the (Executive) Head of School and the Senior Leadership Team is to ensure that staff, in particular, the Head of EdTech and Staff are adequately trained on e-safety and are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

#### 6.2.2. Head of EdTeach

The School's Head of EdTech is responsible for the day to day issues relating to e-safety. The Head of EdTech has responsibility for ensuring this policy is upheld by all members of the school community and works with the EdTech and IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations.

#### 6.2.3. EdTech and IT staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate use to the Head of EdTech and (Executive) Head of School.

**Teaching and support staff**

All staff are required to sign the Staff Acceptable Use Agreement before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture to address any e-safety issues which may arise in classrooms on a daily basis.

#### 6.2.4. *Students*

Students are responsible for using the school IT systems following the Acceptable Use Agreement, and for letting staff know if they see IT systems being misused.

#### 6.2.5. *Parents and Carers*

The school believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about students' behaviour in this area and likewise, it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Student Acceptable Use Agreement.

### 6.3. Education and Training

#### 6.3.1. *Staff: awareness and training*

New teaching staff receive information on e-Safety and Acceptable Use Agreements as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time and are made aware of their responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Agreement, which must be signed and returned before the use of technologies in school. When children use school devices, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be sent by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Head of EdTech and SLT. The School's SLT keeps a log of any reported incidents, including in the student's folder where it pertains to an individual.

### 6.3.2. ***Students: e-Safety in the curriculum***

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to students on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our students' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating students on the dangers of technologies that may be encountered outside the school will also be carried out via Social Skills and ICT classes, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually, via Social Skills and ICT classes, students are taught about their e-safety responsibilities and to look after their online safety. From Year 1, students formally in lessons are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Students can report concerns to the Well-being Department and the Head of EdTech or any member of staff at the school who will report concerns to the relevant person.

From Grade 5 they are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Students are taught about respecting other people's information and images through discussion and classroom activities.
Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Students should approach the Well-being department, the Tutors or the Head of EdTech as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

### 6.3.3. ***Parents***

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about students' behaviour in this area and likewise, it hopes that parents will feel able to share any concerns with the school.
The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school, therefore, arranges annual discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. The last session was held in March 2021; videos of the presentation and the accompanying documentation are sent to new parents and available on request.

### 6.4. Use of school and personal devices

#### 6.4.1. *Staff*

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device that is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the Staff Code of Conduct for further guidance on the use of non-school owned electronic devices for work purposes.

Staff are permitted to bring in personal devices for their use. They may use such devices during break-times and lunchtimes.

Staff working in the early years should note that personal devices MUST be left in the School Office or the staffroom, they are not permitted to be used anywhere in early years areas outside of the school office or staff room.

Personal telephone numbers, email addresses, or other contact details may not be shared with students or parents/carers and under no circumstances may staff contact a student or parent/carer using a personal telephone number, email address, social media, or other messaging systems.

#### 6.4.2. *Students*

If students in Grades 5-12 bring in mobile devices (e.g. for use during the journey to and from school), they should be kept switched off and out of sight all day, following the Acceptable Use Agreement and will remain the responsibility of the child in case of loss or damage. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school has introduced the use of student-owned tablets as a teaching and learning tool, and students are required to adhere to the BYOD Policy when using tablets for schoolwork. In particular, the Acceptable Use Agreement requires students to ensure that their use of tablets for schoolwork complies with this policy and prohibits students from using tablets for non-school related activities during the school day.

The school recognises that mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to use a mobile device for such purposes, the student's parents or carers should arrange a meeting with the Head of EdTech to agree on how the school can appropriately support such use. The student's teachers and other relevant members of staff will be informed about how the student will use the device at school.

### 6.5. Use of internet and email

#### 6.5.1. *Staff*

Staff must not access social networking sites, personal email or any website or personal email which is unconnected with schoolwork or business from school devices or while teaching / in front of students. Such access may only be made from staff members' own devices while in staff-only areas of the school.

When accessed from staff members' devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the Head of EdTech / IT Manager, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to the Head of EdTech / IT Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring the school into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material that is discriminatory or offensive.

Under no circumstances should school students or parents be added to social network 'friends' or contacted through social media.

Any digital communication between staff and students or parents/carers must be professional in tone and content. Under no circumstances may staff contact a student or parent/carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

#### 6.5.2. ***Students***

All students are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure and must be used for all schoolwork. Students should be aware that email communications through the school network and school email addresses are monitored.

There are strong antivirus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, students should contact the IT team for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such communication, to the Head of EdTech / IT Manager / or another member of staff.

The school expects students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Students must report any accidental access to materials of a violent or sexual nature directly to the Head of EdTech / IT Manager / or another member of staff. Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Policy. Students should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work/research purposes, students should contact the EdTech Team and the IT team for assistance (makerspace@park-is.com).

### 6.6. Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
    - Turn off the monitor or minimise the window.
    - Report the incident to the teacher or responsible adult.
- The teacher / responsible adult should:

- Ensure the well-being of the student.
- Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the students).
- Report the details of the incident to the Head of EdTech.

- The Head of EdTech will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

### 6.7. Data storage and processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the GDPR Protection Policy and the Acceptable Use Policy for further details.

Staff and students are expected to save all data relating to their work to the school's Google Drive/ OneDrive.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required to fulfil their role. No personal data of staff or students should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager.

### 6.8. Password security

Students and staff have individual school network logins, email addresses and storage folders on the server. Staff and students are regularly reminded of the need for password security.
All students and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every three months;
- not write passwords down; and
- not share passwords with other students or staff.

### 6.9. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or long term.

When using digital 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 images on the internet (e.g. on social networking sites).

Parents/carers are welcome to take videos and digital images of their children at school events for their personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social

networking sites etc. without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other students in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims but must follow this policy and the Acceptable Use Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Students must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before photographs of students are published on the school website, see Acceptable Use Policy for more information.

Photographs published on the school website, or displayed elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

### 6.10. Misuse

The School will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and other relevant agencies or enforcing authorities. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek external assistance. This includes, but is not limited to, involvement in cyberbullying, 'sexting' or sharing youth-produced sexual images, involvement in radicalisation, grooming and other high-risk activities.

Incidents of misuse or suspected misuse must be dealt with by staff following the school's policies and procedures detailed in the Safeguarding Policy.

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Anti-Bullying Policy.

The iPad usage procedures and misuse of electronic devices infractions can be found HERE.

### 6.11. Electronic Devices - search and deletion

Schools now have the authority to search students for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

The Executive Head may authorise any staff member to search students and to seize anything they have reasonable grounds for suspecting is a prohibited item or is evidence concerning an offence. If a member of staff finds a pornographic image, they should immediately bring this to the attention of the Well-being Department or Executive Head who may dispose of the image unless its possession constitutes a specified offence (i.e. it is extreme or child pornography) in which case it must be delivered to the police as soon as reasonably practicable.

Images found on a mobile phone or another electronic device can be deleted unless it is necessary to pass them to the police. When the person searching finds an electronic device they may examine any data or files on the device if they think there is a good reason to do so. Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The member of staff must have regard to the local regulations and guidelines when determining what is a "good reason" for examining or erasing the contents of an electronic device. In determining a 'good reason' to examine or

erase the data or files, the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. If inappropriate material is found on the device the teacher must consult with the Well-being Department and the Head of EdTech to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

All school staff should be aware that behaviours linked to sexting put a child in danger. Governing bodies should ensure sexting and the school's approach to it are reflected in the child protection policy.

### 6.12. Loading/installing software

For this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free of viruses.
- Only authorised persons, such as the EdTech Team, the ICT Technician or ICT teachers may load software onto the school system or individual computers.
- Where staff are authorised to download software to their laptops/devices, they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

### 6.13. Backup and disaster recovery

The school will define and implement a backup regime that will enable the recovery of critical systems and data within a reasonable timeframe should a data loss occur. This regime should include:

- The use of a remote location for backup of crucial school information, either by daily physical removal in an encrypted format or via a secure encrypted online backup system.
- No data should be stored on the C drive of any school computer as it is liable to be overwritten without notice during the process of ghosting the computers.
- Staff are responsible for backing up their data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.
- Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

The school should also define a whole school ICT disaster recovery plan which would take effect when a severe disturbance to the school ICT infrastructure takes place, to enable critical school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

### 6.14. Guidance on Bring Your Own Device (BYOD) Policy for Staff and Visitors

The school recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and visitors. Our school embraces this technology but requires that it is used acceptably and responsibly.
This policy is intended to address the use by staff members and visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include smartphones, tablets, laptops, wearable technology and other similar devices. If you are unsure whether your device is captured by this policy, please check with the school's IT team. These devices are referred to as 'mobile devices' in this policy. This policy is supported by the Acceptable Use Policy.

### 6.15. Policy statements

#### 6.15.1. *Use of mobile devices at the school (Visitors/Staff)*

Staff and visitors to the school may use their own mobile devices in Staff only areas. Visitors may only use their phones around the site with the express permission of the chaperoning staff member.

Staff and visitors to the school are responsible for their mobile devices at all times. The school is not responsible for the loss or theft of or damage to the mobile device or storage media on the device (e.g. removable memory card) however caused. Reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off when in a prohibited area and at a prohibited time and must not be taken into controlled assessments and examinations unless exceptional circumstances apply.

The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises. Mobile devices may not be used in the early years' areas.

#### 6.15.2. *Use of cameras and audio recording equipment (Visitors/Staff)*

Parents and carers may take photographs, videos or audio recordings of their children at school events for their personal use.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them.

Parents or carers should avoid commenting on activities involving students other than their own in photographs, video, or audio.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school. Staff must comply with the school's social media policy and anti-bullying policy when making photographs, videos, or audio recordings.

#### 6.15.3. *Access to the school's internet connection (Visitors/Staff)*

The school provides a wireless network that staff and visitors to the school may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers to be misusing the network.

An access key to join the visitor wifi may be obtained from the EdTech Team.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's device while using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from the use of the school's wireless network.

#### 6.15.4. *Access to school IT services (Staff only)*

School staff are permitted to connect to or access the following school IT services from their mobile devices:

- the school email system
- the school's student log system (iSAMS)
- school allowed platforms for educational purposes, in exceptional circumstances

Staff may use the systems listed above to view school information via their mobile devices, including information about students. Staff must not store the information on their devices, or cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download school information to their mobile devices to view it (for example, to display an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it.

Staff must only use the IT services listed above and any information accessed through them for work purposes. School information obtained through these services is confidential, in particular information about students. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's IT team as soon as possible.

Staff must not send school information to their email accounts.
If in any doubt a device user should seek clarification and permission from the school's IT team before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

#### 6.15.5. ***Monitoring the use of mobile devices (Visitors/Staff)***

The school may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the school's IT network, staff and visitors to the school agree to such detection and monitoring. The school's use of such technology is to ensure the security of its IT systems, tracking school information.

The information that the school may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content from school IT services or the school internet connection should report this to the school's IT team as soon as possible.

#### 6.15.6. ***Security of staff mobile devices (Staff only)***

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensure that the device auto-locks if inactive for a period.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff are reminded to familiarise themselves with the school's e-safety, social media and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

#### 6.15.7. ***Compliance, Sanctions and Disciplinary Matters for staff (Staff only)***

Non-compliance with this policy exposes both staff and the school to risks. If a breach of this policy occurs, the school will respond immediately by issuing a verbal then written warning to the staff member. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and permission to use the device on school premises will be temporarily

withdrawn. For persistent breach of this policy, the school will permanently revoke permission to use user-owned devices in school.

#### 6.15.8. *Incidents and Response (Staff only)*

The school takes any security incident involving a staff member's or visitor's device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to the EdTech Team in the first instance. Data protection incidents should be reported immediately to the person responsible for the school's data protection controller.

#### 6.15.9. Acceptable Use Policy

This policy applies to all members of the school community, including staff, students, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

### 6.16. *Online Behaviour*

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, material that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or reach the personal email addresses or social media accounts of staff.

#### 6.16.1. *Using the school's IT systems*

Whenever you use the school's IT systems (including by connecting your device to the network) you should follow these principles:

- Only access school IT systems using your username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not try to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

Remember that the school monitors the use of the school's IT systems and that the school can view content accessed or sent via its systems.

#### 6.16.2. *Compliance with related school policies*

You will ensure that you comply with the school's e-Safety Policy, GDPR, Safeguarding Policy and Bullying Policy.

#### 6.16.3. *Breaches of this policy*

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. Also, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the Head of EdTech. Reports will be treated with confidence

#### 6.16.4. Complaints relating to all aspects of E-Safety

As with all issues of safety, if a member of staff, a student or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Please contact the Head of EdTech for further information (jisimas@park-is.com).

## Appendix 1 -Technology Policy and Acceptable Use Agreement

Technology Policy and Acceptable Use Agreement

**The policies, procedures and information within this document apply to all iOS/Windows/Mac devices used in PaRK International School. Teachers and administrators may set additional requirements for use in their classrooms.**

**This acceptable use agreement is provided to make students, parents and teachers aware of the responsibilities associated with the efficient, ethical, and lawful use of technology resources. In the event of any breach to this agreement, student privileges may be terminated and disciplinary action could be applied, in accordance with the PaRK iPad Usage Procedures (effective on the day of breach).**

***All PaRK IS teachers and students are given a Google for Education account that is managed by the school.***

***All PaRK IS teachers and 9th+ students are also given an Office 365 Online account that is managed by the School.***

***All students need to sign and deliver a copy of the Student Pledge before they can use their device at the school. The Student Pledge can be found at the end of this document.***

After reading and accepting the required agreement, students can begin using their iOS/Windows/Mac devices in the classrooms, and if necessary, create and/or continue school work at home.

Internet and device use will be monitored by an institute level administration and software management (MDM) to gauge the use and effectiveness of the device in the classroom. Moreover, contents on the device, including browser history and emails, can be viewed at any time by a teacher upon request.

Teachers reserve the right to restrict device use during class if misuse is suspected. Students must bring their device every day with full battery life to ensure activity for an entire school day, without the need to recharge.

**Purpose**

- PaRK International school´s Technology Policy aims to improve student learning experiences both in and out of the classroom. The school requires students to purchase a personal iPad (Grade 4 to 8) or Windows laptop (Grade 9 to 12) with the expectation that they will make good decisions in regard to personal use of technology.
- Students and Parents/Guardian must carefully read the Acceptable Use Agreement prior to signing it. Any questions should be addressed to the Head of Whole School eLearning Educational Design and clarification obtained before the Acceptable Use Agreement is signed. Signing the document indicates that the student and Parents/Guardian have read and understood the expectations of the school.

**Goals**

- To prepare students for a 21st Century environment
- To increase the productivity and engagement of all learners
- To make student-centred learning a priority
- To increase student collaboration, creativity, critical thinking and communication

**Equipment Grade 4 to 8: iPad**

**Apple ID**

- Every iPad must have an active and verified Apple ID prior to its use on school premises. An Apple ID is a personal account used to access Apple services such as App Store, iTunes Store, iCloud, iMessage, the Apple Online Store, FaceTime, and more, and is available for all users over thirteen years of age. An Apple ID must be created by the Parents/Guardian using the 'Family Sharing' feature of the device or by the student (if already aged 13+).
- Parents/Guardian with a valid Apple ID can use the "Family Sharing" feature to create a Child Account. Parents/Guardian without a valid Apple ID must first create one for themselves before creating one for their child and introducing it to the device. The "Family Sharing" feature can only be accessed on an iOS/Mac device.

**Device**

- PaRK IS recommends the iPad 32GB 8th generation. Students can use another model as long as it is a version equal to or greater than the iPad 6th generation (2018).
- The iPad screen must only be cleaned with approved soft, lint-free cleaning towels. Spray cleaners or liquids should not be used.
- If a stylus is used (optional), it must be capacitive (purchased by the student).
- While the iPad is scratch resistant, the iPad will scratch. Avoid contact with sharp objects. Tempered-glass screen protectors are mandatory.
- Hands should always be clean before using the iPad.
- Food and drink should be kept away from the iPad.
- The iPad must use an approved and appropriate case cover at all times.
- Students must bring the iPad fully charged to school every day. Chargers should be left at home.
- When not in use, the iPad must be stored safely inside the student's school bag.
- The iPad must return to the student's home at the end of each day.
- All material on the iPad is subject to review by school staff.
- All iPads and batteries are covered by the manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the iPad. It does not cover negligence, abuse or malicious damage.
- Families may wish to purchase personal insurance to protect the iPad in cases of loss, theft, or accidental damage. For the iPads acquired through the school, insurance is mandatory.
- All iOS devices must have the "Find My iPad" feature switched on at all times.
- Unless permission is obtained, sound must be muted at all times. Students can use their personal headphones when instructed by the teacher.
- Any problems, vandalism, damage, loss or theft of the iPad must be reported immediately to the Head of EdTech.
- Students will be required to replace lost or damaged chargers/covers.

- All iOS devices that make part of the BYOD Programme must be enrolled in the school's Mobile Device Management system prior to their use on school premises. This process installs an enrollment profile in the iPad that allows the school to manage, secure and update the device. In order for the profile to be installed correctly, the device needs to be restored to factory settings and set up as a new one. This enrollment profile is only removed by the Head of EdTech and the EdTech Team when the student leaves the school.
- Synchronizing an iPad enrolled in the school's MDM system to a home computer is limited to only music and photos. Physical backup can be done on any computer that runs iTunes. For safety reasons, the automatic iCloud backup must be active at all times.
- The iPad's Bluetooth connection must always be kept on when on school premises. Bluetooth is required for the proper functionality of the Apple Classroom app, used by teachers to monitor and manage the students' devices.

**Equipment Grades 9-12: Windows laptop**

**Device**

- The device may be a Windows, MacOS or Linux device. Buying a device model is a personal choice. Ultimately, each Parents/Guardian will need to choose the device that works best for his/her child.
- The device must have the following minimum requirements:
    - Processor: i5 or higher
    - 8GB RAM
    - 256GB SSD
    - NVIDIA/RADEON graphic card
- The device must be able to access a WiFi network. The school has a site wide wireless network for students to use.
- The device must allow the student to be able to type quickly and comfortably. For example, if a tablet/hybrid device is bought then an external keyboard may be useful.
- The screen size and resolution will need to be large enough to work effectively and comfortably all day (suggestion 11'' or bigger).
- The device should have a battery life of at least 6 hours. Students are allowed to charge their devices at school only in exceptional cases, and after requesting permission from a teacher or member of staff.
- The device should be portable and light enough to carry around all day.
- The device must be able to access and create documents with a Google/Microsoft account, such as Gmail/Outlook and Google Drive/OneDrive.
- Providing a padded bag or protective sleeve is suggested. This will provide more protection for the day to day use of these computing devices.
- Device insurance is not mandatory but strongly recommended.

**Phone Usage**

To help Parents/Guardian when collecting students by the end of the day, PaRK INTERNATIONAL SCHOOL allows

students from Grade 5 to bring mobile phones to school, at the owner's risk.

**Incorrect use of mobile phone:** Mobile phones should be kept switched off and in bags or lockers. If a mobile phone is seen on campus before school or at any time during the school day they will be taken immediately. Students can only use mobile phones after they have ended school for the day. If a student needs to make an urgent phone call during school day, they must go to the reception. Any mobile phone taken will be given to the student´s Class Tutor / Head of Year (HoY). The consequences for the use of mobile phones are laid out in the Behaviour Policy.

PaRK INTERNATIONAL SCHOOL will not monitor phone calls and is not liable for any damage or loss of mobile phones.

**Headphone Usage**

**Incorrect use of headphones/earphones/airpods**: Usage of such equipment is allowed in class activities and whenever a school staff has granted permission for its usage. In Senior School, if a student is found to be using this technology without permission then the item will be confiscated and given to the Class Tutor/HOY.

**Student Responsibilities**

The students must:

- Use the device in a responsible, ethical manner and in accordance with the Acceptable Use Agreement.
- Obey general school rules concerning behaviour and communication that apply to the device use.
- Comply with trademark and copyright laws and all license agreements. If unsure, consult a teacher or Parents/Guardian.
- Backup all data securely through iCloud Backup and Google Drive:
    - iCloud Backup Storage comes with 5GB of free storage and is used for backing up purchase history and information, photos and videos, device settings and home screen organization. Students are asked to manage their storage by reducing iCloud backup size, deleting photos or videos, or deleting files stored in iCloud. If necessary, extra storage can be purchased by the student.
    - Google Drive comes with unlimited free storage, as part of the Google For Education programme, and should be used for backing up user-created content, such as pictures, videos, presentations and projects.
- Not create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place. This includes, but is not limited to, removing the Mobile Device Management profile and/or certificates, as well as installing VPN software, hotspot connections and/or unauthorized app managers and synchronous assistants that can allow access to pirated and unofficial apps.

- Not use screensavers, avatars, wallpapers or protective covers that can feature inappropriate or provocative images.
- All profiles for Google Apps and integrated apps that use the school's Google SSO, must be either the school's profile image of the pupil or the default 'no profile image'. The choice is with the pupil.
- Set a security passcode on their device. This passcode should be known only by them to ensure the device is only used by the designated student. The Head of EdTech and the EdTech Team reserves the right to bypass the security code with justifiable reason.
- Keep the device's operating system up-to-date by always downloading and installing available updates. This activity should take place at home to ensure that the device is always fully functional when at school.
- Students are responsible for their personal devices at all times. The school does offer technical support for students having difficulty accessing the WiFi and/or their school accounts. The school takes no responsibility to search for lost or stolen devices nor is there any assumption of financial responsibility by the school for damaged, lost or stolen personal devices.

**Digital Citizenship**

***(applicable to the use of all personal devices)***

The students will:

- Respect the rights and privacy of others.
- Not access, send, upload, download or distribute information that may be considered offensive, profane, threatening, pornographic, obscene, sexually explicit, inappropriate or antisocial inside and outside the school environment.
- Use all modes of electronic communication with integrity, be honest and sensitive to others and reliable in what they communicate. Nothing that is sent through or posted on the Internet can be guaranteed to be private and can be traced, printed off and given to the school or police.
- Not be involved in harassment when using the Internet or other communication devices such as mobile phones at school, at home or at any other location. Harassment is defined as the annoyance to another person or the interference with another person's work. Harassment includes, but is not limited to, the sending of unwarranted messages or messages that are derogatory, defaming or hurtful comments via emails, text messages, posting comments on blogs, social networks, chat rooms or on other websites, SMS or MMS messages and any other modes of electronic communication. If students experience harassment, they should print off the offending material and give it to a member of staff if the incident occurs at school or to their Parents/Guardian if the incident occurs out of school. After discussion with their Parents/Guardian, the incident should be reported to a teacher if the harassment involves other students, teachers or members of the school community. The matter can also be referred to the police.
- Not make comments on the Internet or send comments via SMS, MMS, memes or other means of electronic

communication that could hurt the reputation of the school.

- Not use the school's Internet network for chatting or sending messages under any circumstances without the consent of a teacher. Any internal or external communication is only allowed after the completion of the school's daily schedule.
- Not reveal personal details while on the Internet, including email accounts, passwords, home address or phone number, or the address or phone number of others.
- Be aware that information published on the Internet may be inaccurate or may misrepresent a person or situation.
- Not plagiarise or violate copyright law.
- Not impersonate others when using the Internet.
- Not log in using someone else's account.
- Not remove, edit or replace their Apple ID for any reason, without the consent of the school and/or their Parents/Guardian. Any changes to these accounts must be immediately reported to the Head of Whole School eLearning Educational Design.
- Notify the Helpdesk and the EdTech Team department if they identified security or any other problem with the school's network.
- Use social networking sites in a responsible and cyber safe manner by not revealing personal details, by limiting access to their social networking pages to people whom they know and can trust and by not posting offensive or harassing information on websites.
- Act responsibly when taking photographs and videos, sending them using electronic devices and posting them on the Internet. It is expected that students will:
    - Not take photographs or videos at school or school-related functions or activities without the permission of the teacher.
    - Not distribute or post photographs, graphical images or videos of students, teachers or their relatives on the Internet without their permission.

**Parents/Guardian**

- Parents/Guardian is responsible for supervising their child's use of the device when not in school.
- Take extra steps to protect your child:
    - Encourage your child to use and store the device in an open area of your home, such as the kitchen or family room so you can monitor what your child is doing online.
    - Use the Internet with your child to help develop safe surfing habits. Children often model adult behaviour.
- Go where your child goes online:
    - Monitor the places that your child visits.
    - Let your child know that you are there, and help teach them to act appropriately as they work and

socialize online.

- Review your child's friends list.
- Report unwelcome or malicious online threats.
- Help your child develop a routine in the use and care of the device.
- Take a look at the apps or programmes installed and try to have a working understanding of the programmes and student work found on the device.
- Read and share the PaRK International School Acceptable Use Agreement to create a clear set of expectations and limitations for your child.

**STUDENT PLEDGE**

- I understand that the care of my device is my responsibility.
- I will never leave my device unattended.
- I will ensure that my device battery is charged nightly.
- I will protect my device by keeping it in an approved case at all times.
- I will keep food and beverages away from my device as they may cause damage to the device.
- I will avoid using objects that may scratch the screen.
- I will not expose my device to extreme temperatures and direct sunlight.
- I will not delete any school installed applications, certificates, profiles or software.
- I will be responsible for my behaviour when using the Internet. This includes the resources I access and the language I use.
- I will use my device in ways that are educational, appropriate, polite and sensible.
- I will follow the school's Acceptable Use Agreement at all times.
- I will follow and respect the classroom rules concerning device usage.
- I understand that my device is subject to inspection at any time without notice.
- I understand that my use of the Internet and other related technologies may be monitored and logged and can be made available to my teachers.
- I will be responsible for all damage or loss caused by neglect or abuse.
- I will only use my device in school, including the internet, email, digital video, mobile technologies, etc. for school purposes.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.
- I will not attempt to bypass the internet filtering system.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my Parents/Guardian may be contacted.

Dear Parents/Guardian,

We expect all students to be safe and responsible when using their iPads. It is essential that students are aware of the rules and know how to stay safe when using technology at school and at home.

Students are expected to read and discuss the PaRK International School Acceptable Use Agreement with their Parents/Guardian and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with the Mobile Device Admin.

Student's Signature _____

Parents/Guardian's Signature _____

## Appendix 2 - Staff Laptop/Devices Acceptable Use Agreement

1. **Introduction**
   - This agreement applies to all laptops and other associated devices that are loaned to staff and therefore remain the school's property.
   - It should be read in conjunction with the school's e-Safety Policy
   - All recipients and users of these devices should read and sign the agreement.

2. **Security of equipment and data**
   - The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
   - Staff should understand the limitations of the school's insurance cover.
   - Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

3. **Software**
   - Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
   - The only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
   - Users should not attempt to make changes to the software and settings that might adversely affect its use.

4. **Faults**
   - In the event of a problem with the computer, the school's ICT Technician/Network Manager should be contacted.

**Declaration:**

I have read and understood the above and the school's e-Safety Policy and agree to abide by the outlined rules and requirements.

| | |
|---|---|
| Name: | |

| | |
|---|---|
| Signature: | |
| Date: | |

## Appendix 3 - Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, and social networking. ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Executive Head.
- I understand that my use of school information systems, the internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security, and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of students, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely following the school e-Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with students (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that student use of the internet is consistent with the school's e-Safety Policy.
- When working with students, I will carefully monitor and scrutinise what students are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to monitor what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer (delete/put it on the garbage and report it immediately to the EdTech Team or the IT department - makerspace@park-is.com).
- I will report any incidents of concern regarding students' safety to the appropriate person, e.g. Head of EdTech and SLT member (jisimas@park-is.com).

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes the unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

**Damage or Loss**

Teachers have the responsibility to immediately report any damage or loss to the EdTech Department (makerspace@park-is.com) and to the IT department to determine the necessary action. It is the responsibility of the teacher to take care of the device without loss, negligence or abuse. **Loss or damage of the device may require substitution for a new device and the Teacher may be required to cover the cost of the damage or loss of the device (190-250€ depending on model type).**

I have read and understood the above and the school's e-Safety Policy and agree to abide by the outlined rules and requirements.

**Name:** _____ **Section/Campus:** ☐ ELS ☐ LWS ☐ UJS ☐ SS

**iPad serial:** _____ **Materials:** ☐ iPad ☐ Charger ☐ Case/película ☐ Others

**Date:** _____ **Signature:** _____

Delivered by the EdTech Team :_____

## Appendix 4 - Rent Your Own Device Agreement

**iPad Lease Contract (2021/2022)**

New students enrolled at PaRK International School for Grade 8 can rent their own device for an annual fee, not refundable, for the purposes of facilitating education, should they decide not to buy their own device (from Grade 9 students should use a laptop). The rental plans available are:

| Device | Extras included | Annual rental fee |
|---|---|---|
| Apple iPad 8th Generation (2020) | Glass Screen Protector | 250€ |
| Apple iPad 7th Generation (2019) | Glass Screen Protector + UAG Hardcover | 190€ |

The School leases the iPads on behalf of its students for one year (3 terms); the iPad must be returned upon a student withdrawing or graduating from the school. The School retains all ownership rights of the iPad; the School may inspect the iPad and all stored information at any time with or without notice, and the student should not have an expectation of privacy as to anything stored on, sent by, or received through it. At the end of the third term, students will return the iPad to the school, and all personal data will be deleted.

**Customization**

Any preference settings, such as the wallpaper, screen brightness, or location services, may be changed by the student. The purchase of some apps will be required by course instructors, and with their parent or guardian's permission, students have the option to buy other apps from the Apple iTunes Store and download them to their iPad. Hacking or jailbreaking an iPad is not allowed; if a student's iPad is found to be hacked/jailbroken or if it is deemed that the iPad is being used inappropriately in any manner, the student will be subject to disciplinary action and possible financial penalties associated with harming the device.

**Damage or Loss**

Students should report any damage or loss to the EdTech Department, which will determine necessary action. All iPads are covered by a warranty that covers the manufacturer's defects. The warranty does not cover loss, negligence, and abuse. For example, carelessly dropping the iPad, throwing the iPad, or using the iPad as an umbrella would be considered examples of neglect and abuse.

Students pay an annual fee of 190€ or 250€, depending on the rental plan selected, not returnable, which will cover the first incidence of damage or loss. See the section below, Financial Responsibility, for further details.

**Standards for iPad Care and Use Student Responsibilities**

- Bring the fully-charged iPad to school every day.
- Keep the iPad with you or within your sight at all times.
- Keep the iPad secure in its protective case or covering, ensuring that corners are covered properly and do not remove it.
- Other than parents or guardians, do not let anyone besides yourself use the iPad.
- Read and comply to the Technology Policy and Acceptable Use Agreement
- Report any problems, damage or theft immediately to the EdTech Department.

- Create a Passcode on the iPad and keep the Passcode confidential.
- Any apps or data stored on the iPad must be consistent with school policy and the Mission and spirit of the school.

**General Care**

- Do not do anything to the iPad that will permanently alter it in any way.
- Do not remove any serial numbers or identification placed on the iPad.
- Keep the equipment clean. For example, do not eat or drink while using the iPad.
- Clean the screen with a soft, dry anti-static cloth or with a screen cleaner designed specifically for LCD type screens only. Do not use paper towels, which may scratch the screen.

**Personal Health & Safety**

- Take frequent breaks when using the iPad for long periods of time. Look away from the iPad approximately every fifteen minutes and focus on a distant object to prevent eye strain. Keep track of how long you spend using the iPad.
- Do not provide your personal information to anyone over the Internet.
- Do not share your passwords with anyone.

**Financial Responsibility**

Students pay an annual fee of 190/250€, not returnable, which will cover the first incidence of damage or loss. Subsequent damage will be repaired by the School when possible, and the cost billed to the student. In the case of a second iPad's destruction or loss, the student will be billed for the full value of the replacement iPad, 420€.

**Signatures**

| Student name | Signature | Date |
|---|---|---|
| _____ | _____ | _____ |
| Parent/ Guardian name | Signature | Date |
| _____ | _____ | _____ |

Last reviewed:May 2021

Reviewers: Heads of Cycle | Heads of School | Barbara Lancastre | Marta Pereira

Next review date: May 2022