Good Will Children Private School
Integrated ICT Policy

School Vision and Mission

Vision

Empower students to develop a growth mindset and reach their full potential through collaboration, exploration, and citizenship, so they can impactfully contribute to the global community of a changing world.

Mission:

- GCPS develops the content knowledge, skillset, and ethics to make positive global citizens, true innovators, and passionate leaders.
- GCPS cultivates a deep understanding of Islamic values and the culture of the UAE to develop a character that is identified by integrity, self-discipline, and tolerance.
- By promoting a learning environment of academic excellence and building strong partnerships with families and the wider community, we prepare students to be lifelong learners with high expectations and an appreciation for diversity.
- To provide broad and balanced learning opportunities that enable students to experience rich language acquisition and reach their full potential.

Adopted on: July 2022
Revised on: August 2023
Review Date: August 2024

Distribution List

Principal /Board of Members
School Heads
Academic Staff
Administration Staff
Parents

➢ Purpose of Policy:

ICT has been an inevitable part of our everyday lives and at Good Will Children Private School, we take this area to build the holistic development of child to cope with the challenges of 21st century and at the same time to equip them with better technology tools across teaching and learning throughout our school.

Our Cambridge Curriculum of Information and Curriculum Technology already provides with rich content to help our students for lifelong learning which includes strands of computational thinking, programming, managing data, networks and digital communication and computer systems. In order to provide the broad and balanced curriculum ensuring that our students use technology as medium to explore the world, think logically and become responsible, innovative, confident and reflective learners, we aim to do;

- To raise students' competence and confidence in using ICT by developing their knowledge, skills and understanding in using a wide range of ICT tools
- To enable students to meet the requirements set out within the Cambridge curriculum and to develop them into responsible, innovative, confident, engaged and reflective learners.
- To raise levels of teacher competence and confidence in integrating ICT into their daily planning, teaching and assessment.
- To provide equal access and opportunities in ICT for all students', regardless of age, gender, ethnicity with our vision and fulfilling that with the use of smartboards in classrooms, providing laptops and tablets to students, access of cellular wireless networks with latest technology platforms.
- To develop students' independent learning skills using ICT across all areas of the curriculum both in school and at home
- To harness the power of technology to help people of determination to increase their independence and develop their interests and abilities

➢ Policy Framework:

ICT is an area that continues to accelerate and intensify year on year and at GWCPS and our students have reached new heights of technology by participating in various internal and external competitions.

The technology is also been seen as integrated with thematic learning from KG 1 to Grade 2 providing opportunities of learning with lots of fun activities along with the interactive games to reinforce math, spelling, phonetic, and reading skills along with the Cross Curricular integration from Grade 3 to 8 where students learn to use the web blog and website to reach wider

audience. Our students use multimedia skills to present their work in various subjects, projects are designed with the use of online technology tools, learning was not affected during pandemic where our teachers used the technology to transform their learning into more exciting and challenging through the use of Classe365 LMS, online stimulations, virtual labs, virtual trips and interactive software.

The focus on Using ICT means that students have opportunities to transfer their knowledge, understanding and skills in a variety of meaningful contexts across the curriculum.

Access of Resources

At Good Will Children Private School, we seek to provide staff and students with an ICT rich environment and we continually invest in new, current and up to date ICT facilities. The school maintains and develops a range of ICT equipment including:

- Classroom Computers for teachers
- Laptops access for students and teachers
- iPads for students
- Interactive whiteboards in classrooms
- Data Projectors in classrooms
- Colour and black and white printers
- Bee bots
- Lego robot kit
- Sensory boards used in EYFS play area
- Technology support softwares such as Classe365 LMS, Reading A to Z and I Start Arabic.

In order to maximize the use and benefits of the school's ICT facilities, GWCPS aims to make the ICT facilities available:

- to every child through an iPad along with our BYOD policy to support learning through technology.
- in various classrooms as a tool to produce work and research information
- in each class to be used by the class teacher as a learning and teaching aid
- All students have access to the Classe365 LMS to check their daily message from teacher, check their homework, refer to learning material within that week and also do assessment online.
- All students have supervised access to internet

Planning and Monitoring

Whole School Level

- Principal and MLT team will consult on how ICT is incorporated into the School Development Plan
- ICT is then integrated into English, Maths and Science primarily by agreed Long term and Mid-term planning
- KG1, KG2, Grade 1 and Grade 2 follow the thematic learning where ICT learning objectives are embedded in their learning theme.
- Cambridge scheme of work for ICT is followed by ensuring the progression and continuity for students from primary and lower secondary.
- Grade 3 to 8 takes the ICT learning objectives and use in developing projects, participating in various internal and external STEM competitions.

Class Level

- ICT will be embedded into all areas of the curriculum within all subjects through daily lesson plan.
- ICT with be planned for whole year basis (Long term) , termly basis (Mid term) and weekly basis (Short Term).
- KG to Grade 2 works on thematic learning with integration of all subjects in one common theme. Grade 3 to 8 incorporates the cross curricular links which is clearly mentioned in daily lesson plan and is also integrated in lesson material.
- Each class is equipped with Smart board and projectors along with the iPad access to students which integrates the technology streamlined into lessons and assessments.

Implementation

Coordination

At Good Will Children Private School, we believe that it is important that if ICT is to make a valuable contribution to the learning and teaching throughout the school:

- There should be a consistent approach to ICT throughout all of the Key Stages
- All staff (teaching and non-teaching) should have in-school help, advice and training
- The school should be kept up to date with new developments
- Learning should be monitored to ensure coherence and progression
- Learning in the Classroom using technology is used by laptops, iPads and interactive whiteboards where online videos, using Zoom to facilitate the online students, online websites, use of Google drive for the students and staff folders, use of purchased softwares like Reading A to Z, and I Read Arabic.
- E safety concepts of digital responsibility, Cyberbullying and plagiarism is reinforced in health and safety week in Term 1 of each academic year

The member of staff appointed to coordinate ICT is the ICT teacher.

The Role of the Principal

The principal discusses the role of integration of ICT with ICT Lead and ICT teacher before the start of each academic year. T

The principal, in consultation with the ICT coordinator and staff will:

- Determine the way ICT should support, enrich and extend the curriculum throughout the school – Due to COVID 19 and remote learning the Principal and ICT Lead have devised a distant learning policy to run alongside the BYOD, Data protection policy and Online safety policy which supports e-safety and acceptable use policy to ensure that ICT is still used to support and enrich curriculum during school on distance learning.
- Decide the provision and allocation of ICT resources – IT Officer has to log on every ICT resource in ICT inventory every term and also keeps the provision of logs.
- The use of ICT resources are monitored regularly by IT officer and principal to ensure that data protection and safety of all students and staff are well maintained.
- The health and safety week is conducted in Term 1 every year to enrich the content of E safety and Cyber bullying concepts to students and to behave as a responsible digital citizen.
- The school supports student learning by incorporating the reading platforms in their daily learning activities. To ensure that teachers motivate and guide students on regular basis in their lessons with the integrated technology.
- To review ICT policies and its safety and hazards on regular basis and make proper amendments.
- The library is using the full potential of technology in library lessons to ensure that students use technology to research and innovation.
- Develop the School Development Plan based on the ICT need based analysis and action plan with ICT lead and ICT teacher to incorporate ICT with whole school.

The Role of the ICT Lead

It is the role of the ICT Lead to:

- Liaise with the ICT teacher and Principal in the drawing up of an ICT policy for the whole school
- Liaise with the Principal and ICT teacher in the drawing up of long term, Mid term and short term planning that integrates the ICT learning objectives within all subjects.
- Ensure that ICT is included in school policies and schemes of work for various curricular subjects
- To provide leadership and direction for ICT as necessary with the Cambridge Curriculum scheme of work
- Based on the need-based analysis, draw an action plan that incorporates the ICT integration in professional development of staff.
- Attend courses relevant to personal training and development

- Motivate the students to participate in various STEM competition both within and out of the school

- Make staff aware of the health and safety aspects of ICT and ensure that these are included within the school's online safety policy
- Monitor the work being carried out in the area of ICT in the various Key Stages to ensure progression
- Review the policy of distance learning , BYOD and Online Safety on regular basis

The Role of the classroom teacher

It is the role of the ICT teacher to:

- Integrate ICT into their curriculum planning, classroom teaching and assessment of student's work
- Ensure that any ICT resource used within the classroom is appropriate to curriculum needs and the needs of the children within the class – follow the skills and learning outcomes as set out for each year group in the lines of progression and scheme of work with Cambridge Curriculum
- Plan for cross-curricular and creative use of ICT resources and learning outcomes

Staff Development

Good Will Children Private School facilitates staff development in ICT by:

- Giving all staff opportunities to attend relevant ICT topics such as QR code, Online technology tools, Excel training in data analysis etc
- Giving staff who have attended courses opportunities to share the experience gained with other staff (The peer CPDs are usually conducted during Mid term holidays where one week is dedicated to staff for CPD development)
- Setting sufficient time aside to allow teachers and teacher assistants opportunities to enhance their ICT skills
- Conducting ICT survey of skills with teachers to identify the technology need trainings

Assessment

At Good Will Children Private School, all our assessments (both summative and formative) are conducted online. It is the role of class teacher and IT officer to ensure that assessments are conducted through the use of online technology tools and the learning management system to check the student understanding and setting up the targets.

Teachers use mentimeter, Kahoot and other online tools for meaningful and timely feedback to students.

Class organization and teaching style

At GWCPS the teaching of ICT takes place within the classroom using iPads and laptops. Students are grouped sometimes by ability (mixed or similar). Software or a specific skill might be introduced to a class or work set for a particular child, depending on the task.
ICT is a cross curricular tool so it is linked to all areas of the curriculum. ICT also provides learning and teaching cross the following cross curricular dimensions:

Using iPads

At GWCPS we realize the power and potential of the iPad as a great tool for learning. The iPad brings a new way for lesson delivery and engagement with students. The iPad is a superb learning tool especially in relation to critical thinking, problem solving, decision-making, research and information fluency. It stimulates creativity; it encourages learning and it enables great challenge centered lessons.

IPads are used in a range of ways appropriate to the age and abilities of the pupils as they progress through the school. The school has iPads which work on a weekly timetable so as all classes get sufficient time with the iPads. Each teacher also has their own laptop and desktop computer in classroom to access technology.

Teachers should remember that the use of iPads needs to be planned for, not just used to set in front of the children and let them play 'games' as a time filler. The iPads all have a range of Apps on them and many of them are open ended, creative Apps where the content is not the issue, but rather the skills and creativity that they promote (Book Creator, iMovie, Scratch Jr, etc.)

Teachers should be aware of security with the iPads and not leave them sitting out on desks at break and lunch times. Moreover it is the duty of the teacher assistants to ensure that iPads are sanitized after every use and is handed to IT officer by signing the lending sheet.

Equal Opportunities

All teaching and non-teaching staff at GWCPS are responsible for ensuring that all children, irrespective of gender, ability, ethnic origin and social circumstances, have access to the whole curriculum and make the greatest possible progress in all areas of the curriculum while at our school.
ICT is an area of the curriculum where, because of its unique nature in requiring specific equipment, equal access needs to be planned and monitored very carefully. It is the

responsibility of individual teachers to organize their pairs and groupings so that this is achieved.

Technology for People of Determination

All children should have access to a broad, balanced curriculum that includes ICT, and they should make the greatest progress possible. Provision for children with SEN in relation to ICT is the responsibility of the class teacher, Support Staff and SEN Co-ordinator as appropriate. ICT, especially, provides a means whereby children with SEN are able to present and develop their work more easily.
- When possible, ICT equipment is made available for a specific child, or groups of children to work with Support Staff and/or work with each other, so that work can be drafted and redrafted.

- Procedure:

- Good Will Children Private School has a robust Firewall Analyzer that collects and archives the log obtained from proxies, analyses and generates useful internet access information system. The filtering system blocks all harmful and malicious websites including social networking websites such that students are protected from moral values of Islamic and UAE culture values.
- The top talker report that is generated by the Firewall Analyzer is able to monitor student's internet usage and the details of the conversations that has taken place between source and destination.
- The school IT department uses website details report from Firewall to monitor and track the most frequent visited websites, domains and web pages. The IT department uses the pattern generated to regulate the types of websites used by students and staff.
- The school has strong hold of denial of request from any unauthorized server or webpage which makes it safe and secure for students to access internet and to protect them from online materials that are not consistent with morality, decency or public order.
- As the user does not have direct access to proxy server level, the staff and students are not been able to download any harmful or inappropriate material from the internet.
- The School supports student learning by incorporating various software in their daily learning activities. The teachers motivate and guide students on regular basis in computer lab to challenge their mental level and to support their learning outcomes.
- The School has proper internet policy guidelines and conducts regular workshops for students to educate about the safe internet access and cyber bullying.
- Currently school operates two login accounts. Account-1 is an admin login and Account-2 is a guest/teacher login. If there will be any attempt to download harmful software to computer by any user than system will automatically request admin password for credibility and

authentication purpose. The passwords are only known to IT department and thus no user can download malicious software that is unauthorized.

- All our teachers and librarians are trained to play an active role in guiding dangers of the internet and monitoring websites accessed by the students in school and during school trips.
- Good Will Children School
- is actively involved in guiding and educating students in online activities that will support learning outcomes, depending on student's age and maturity. The school has also made student pledge as being signed by parents to understand the school internet responsibility for students.
- The staff and parents have educated through this policy to be take preventive measures for email attachment and to access from private and secure network.
- The school is currently using the Kaspersky 2016- 2017 Antivirus software on school devices to protect it from any malware or virus.
- The school has one main server in telephone room which handles all the student information and data on hard drive and refrains to publish on website. Only IT personnel and authorized person can access the data.
- As a responsible school and community in UAE, it values and respects the UAE cultural aspects and has followed and agreed the TRA (Telecom Regulatory Authority) guidelines in blocking following websites. The school also abide with moral obligations of culture and tolerance (also refer to UAE cybercrime Law No. 5 of 2012).
    - *Internet Content that contradicts with the ethics and morals of the UAE including any adult literature or images.*
    - *Internet Content that contains material which expresses hate to religions and offensive to Islamic culture.*
    - *Internet Content that is not in line with UAE Laws.*
    - *Internet Content that allow or assist users to access Blocked Content.*
    - *Internet Content that directly or indirectly constitute a risk on UAE internet users such as Phishing websites, Hacking tools & Spywares.*
    - *Internet Content that is relevant to gambling.*
    - *Internet Content that provide information on purchasing, manufacturing, promoting and using illegal drugs.*

➢ Cyberbullying

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior.

The most common places where cyberbullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and TikTok
- Text messaging and messaging apps on mobile or tablet devices
- Instant messaging, direct messaging, and online chatting over the internet
- Online forums, chat rooms, and message boards, such as Reddit
- Email
- Online gaming communities
- Sending, sharing or posting nasty, hurtful or abusive messages
- Humiliating someone by posting/sharing embarrassing videos or images
- Tagging someone inappropriately in an image
- Spreading rumors or lies about someone online
- Trolling - saying mean things to incite people up against someone
- Imitating someone online
- Making threats towards someone online
- Sending repeated harassment and threatening messages (cyberstalking)
- Deliberately excluding someone from a group/conversation

Report incidents: If you find yourself aware of any similar situations where someone is being subject to cyberbullying, you should report such incidents to school social worker immediately. Although you can report to your class teacher, make sure you know how to contact the social worker.

➢ Cyber Safety Guidelines

The Internet is an incredible platform for children to learn, express themselves and have fun, but it also has its dark side. Not everything on the Internet is safe and can be trusted. Even though the benefits outweigh the potential dangers, parents and guardians must be aware of the real risks that children may be exposed to online.

Top tips for Parents to keep children safe online

- **Educate**

It is important that you are aware of your child's Internet activities including the social media channels they utilize, games or other online activities they are involved in. Being aware of your child's online activities will help you identify possible threats to educate and advise your child accordingly. It is important that children understand the impact that their online activities can have on themselves and others, today and in the future.

- **Protect**

There are parental control tools available to help protect your children from harmful and inappropriate online content. Phones, tablets, game consoles and other devices that connect to the Internet have parental control settings. Technology can be effective, but no system is 100%

fool proof, so education remains key.

- **Monitor**

Keep an open dialogue with your children about their use of Internet. Younger children should only use the Internet when they are in a family area so you can monitor what they are doing and how they are using it. As they grow up they will demand more privacy, but it's important to stay interested and engaged.

- **Support**

Make sure your children know they can talk to you if something goes wrong online. You also need to know how to respond to these situations. Most websites now have "report abuse" buttons where you can report inappropriate behaviour.

Parent Note

Please teach your children the safeguards for the above scenarios and ensure they follow the below guidelines in cases where bullying might be happening:

- Notify a parent or guardian (someone whom you trust) about the incident immediately
- Don't respond, forward or delete any of the offensive messages
- Obtain screenshots and gather as many details as possible about the profile that has been sending offensive messages
- Tell your teacher / Social worker or other trusted adult as soon as possible.

➢ Guidelines on Audio/Video Conferencing

DO's

1. **Safeguard your personal information**: Your surroundings (items in the background which are in focus within the screen) could reveal a lot about you. e.g. school uniform, identity cards, neighborhood that you are in etc.
2. **Adjust security settings**: Review the security settings of the tool you are using and disable features that may be harmful or are not in use.
3. **Keep your password in secret:** Avoid sharing your passwords with other people as they can use them to act on your behalf.

DON'TS

1. **DO NOT Record/livestream people without their consent:** Recording the lectures on live sessions (Microsoft TEAMS and ZOOM) is strictly NOT allowed.
2. **DO NOT Share inappropriate content or use inappropriate language**: Some of your messages could be offensive for other people in the conference. Think twice before you send anything to group or personal chat.
3. **DO NOT invite external participants:** Do NOT invite any other student and share

personal chats on Microsoft TEAMS and Zoom.

➢ Guidelines on Internet Browsing

DO's

1. **Beware of pop-up scams:** Most pop-up advertisement campaigns that appear when you browse are scams. Some may also trick you into installing malware (damaging software) on your computers.
2. **Be careful of sharing your details:** Some online services may collect and sell your personal information (including credit card details) to third parties. Refrain from sharing your personal details unless you are confident of the web platform being used.

DON'Ts

1. **DO NOT access illegal sites:** Accessing such sites or using file-sharing programs that offer free downloads of movies, music or software can expose your system to malware, violent or inappropriate images. You could also be breaking the law or committing copyright violations.
2. **DO NOT Save your passwords in the browser:** Doing this could leave you more vulnerable to being hacked.
3. **DO NOT use VPN (Virtual Private Network)**

Parent Note

Make sure your child consults with you before signing up to a new online forum, social media platform or any other service over the Internet.

➢ Guidelines on Device & Online Services Security

DO's

1. **Ensure you install a trusted Anti-Malware:** This software will protect your system from majority of common computer threats. Don't forget to keep it up-to-date with product updates.
2. **Make use of parental controls:** Parental control settings are available in most of the modern smartphones and tablets. There are many parental controls available in the market to access.
3. **Secure your wireless network:** Reset the router password so it follows good password rules and isn't easy to guess and enable wireless encryption to prevent a stranger from spotting your network from the Internet.

DON'TS

1. **DO NOT turn off security software:** Software such as anti-virus scanner or firewall should never be turned off.
2. **DO NOT install pirated or illegal software**: Pirated software may come cheap but you will have a hidden cost on your privacy and computer security. Always use genuine software.
3. **DO NOT use unknown Wi-Fi networks**: Data exchange between your computer and Internet can be intercepted and monitored by a cyber-criminal. Never use public Wi-Fi to access your financial data.

Parent Note

Tell your children not to turn off the virus scanner or firewall, even if they think it might speed up a game. It's just not safe to take this risk.

➢ Guidelines on Social Media & Online Communication

It is easy for cyber-criminals to create fake accounts and use them for illegal purposes. Remember, all people that you meet online are strangers, no matter how long you may have known them or how friendly they appear to be.

DO's

1. **Review your privacy settings:** Ensure your social media accounts and privacy settings are configured to be restrictive, so that your posts and personal details are only revealed to your friends and not strangers. Review your privacy settings periodically.
2. **Think before you post:** Whether on social media website, mobile apps or any other online platforms. Always take a minute to think before hitting the "Send" button.
3. **Report immediately**: If someone is making you or your child feel uncomfortable by being abusive or inappropriate, or pressurizing you or them to do uncomfortable things, block and report the user on the platform. Social networking sites provide a reporting option which you should familiarize yourself with.
4. **Use your account only**: Use your own account for Microsoft TEAMS and Zoom online sessions and on Classe365 LMS.
5. **Share your concerns with the school**: The students are requested to contact the school social worker directly in case of any online concerns and queries.

DON'TS

1. **DO NOT share your school information online:** The school has dedicated people who are authorized to share any school related information online
2. **DO NOT share your personal information**: This includes your home address, phone numbers, bank details or anything that should be known only to you or your family members.

3. **DO NOT accept friend requests from strangers**: Many requests are made from fake accounts and may be from people who have constructed fake personal profiles that do not reflect the reality.
4. **DO NOT meet someone you have come to know online: The** person may not be who they claim to be and meeting them offline can pose risks.
5. **DO NOT post, share, trade your pictures/videos:** This especially applies on embarrassing content or content you would not want others to see. Once you have shared the content on Social Media, online forums, website or anyone over the Internet it cannot be undone.
6. **DO NOT tag or post pictures of others without consent:** This includes your friends, just as you would not want someone posting or circulating pictures of you without your permission.
7. **DO NOT post offensive content:** Some topics such as someone's religion, race, organization or a community could upset people and may also be against the law or in breach of the social media platforms' usage terms – avoid posting such sensitive content.

Parent Note

Make sure your child is aware of all the recommendations listed above and follows them while browsing the web.

➢ Guidelines for Sending and Receiving Email

Nowadays, cyber-criminals may try to trick you into revealing your personal information and passwords by means of email, messengers, SMS or voice calls. You should be suspicious of any messages that try to scare you into opening an attachment or logging into the website to verify your account or reset your account or request personal details etc. we request all our students and parents to not respond to such messages or act on their instructions.

DO's

1. **Verify Sender**: Always verify the sender and the organization (the part after "@" sign) you have received the message from. If you receive an email from Good Will Children Private School, consider verifying its authenticity from the school directly.
2. **Verify the links**: Always verify the link before clicking it. You can understand the real link destination by hovering your mouse cursor over it.
3. **Mark suspicious emails as Spam**: This will protect you from similar messages in the future.

DON'TS

1. **DO NOT click the links**: If a message seems suspicious, do not click the links embedded in it.
2. **DO NOT reveal your personal information**: Do not respond to messages that request

your usernames/password or personal information about yourself, your friends and family.

3. **DO NOT open Attachments**: Do not open attachments in emails you were not expecting to receive.

➢ Guidelines on User Accounts & Passwords

DO's

1. **Select a strong password:** Your password should include a combination of upper case, lower case, number and special characters.
2. **Change your password regularly**: Update your password from time to time, especially if you suspect that the password may have become known to someone.
3. **Always logout:** When you are finished with your activity don't forget to press "Logout". Especially while using public Wi-Fi networks. Remember, someone can misuse your account and send messages on your behalf.

DON'TS

1. **DO NOT Reuse Passwords:** Always create a new unique password for every account you create online.
2. **DO NOT Share your username/password**: Don't tell your password to anyone including your family members, friends and peers.
3. **DO NOT write down your password:** They can be easily spotted and used by other people.
4. **DO NOT use your personal data in a password**: Never include your name, birth date, spouse name, pet name etc. as a part of your password

Parent Note

Make sure you have your child's passwords for email, messengers and social networking sites. It's a good idea for you to review who is communicating with your child and in the event of trouble, you'll have important access.

➢ Guidelines for Parents to Monitor their Children on Distance Learning

- Place the laptop or computer in a identified area in your home within your supervision.
- Frequently check the exchange of information like messages and materials between your child, their peers, and the school or third entity.
- In case of any wrong suspicion activity on internet or during Microsoft TEAMS and Zoom sessions, report it to school social worker.
- Have frequent conversations with your child regarding online session experiences.

- Install the parent control software to monitor your child's online activities.
- Use only your account for online sessions (Microsoft TEAMS and ZOOM) and Classe365 LMS.

➢ Guidelines for Bring your Own Device (BYOD)

- Learning about and being held accountable for the responsible use of electronic and digital tools is an important part of preparing students to be successful in today's knowledge society. Personal electronic devices are the sole responsibility of the student owner. The school has no responsibility for these personal devices if they are lost, loaned, or stolen.
- Electronic devices must be used in a manner consistent with the Good Will Children Private School's Safe Internet Guidelines and the school reserves the right to limit use of electronic devices, especially when these devices are used to harass others or disrupt the learning environment
- Students must use their tablets and laptops from home in the ethical way.
- Students will obey all safe internet guidelines of school like behaviour and communication while using their own technological devices.

➢ Strategies for the safe practice of internet

- To conduct workshop for parents about awareness of cyber bullying and encouraging their child in safe usage of internet practice.
- To assign the E safety coordinator among students that encourages the good practices of internet usage among students.
- To involve the student council members in raising the awareness of cyber bullying and internet practices.
- To regular review the Online Internet Safety policy and update the staff about important aspects of internet security.
- Teachers need to conduct the inter class competitions to support E-learning with motivating them by giving house points.
- The promotion of this policy will be done in SLT meetings, arranging workshops for students and staff, parental involvement, computer lab posters and internal circulars.

➢ Responsibility of All staff

Acceptable Uses of School's Internet by Staff:

- All the staff of Good Will Children Private School L.L.C. are advised to use internet only for the work or study related matter.

- Teachers and administration staff are responsible to protect the student data and keep it confidential and secure all times.
- Teachers are responsible to educate students about awareness of malware advertisements in email attachments and not to download from suspicious source. In addition all staff are advised to open the email from private and secure network only and do not respond to suspicious and tricky advertisements.
- Teachers are responsible to allow monitoring of internet access to students for educational purpose only. Staff should conduct themselves professionally online and are STRICTLT NOT allowed to access social networking sites or shopping websites during school operational hours.
- Teachers are responsible to use only educational related material in classrooms and should not play any videos or songs not related to educational activity.
- Teachers are advised to be vigilant and educate students on not sharing passwords or email information with anyone.
- Teachers should integrate the ICT in their teaching subjects to enhance the ICT skills and competencies of students.
- Ensuring that no staff can access the internet by any unauthorized means of log in.
- Teachers should promote the good teaching practices though supporting student's learning in all aspects like projects, integrated teaching and E learning software.
- All staff are responsible for their data and the devices that they bring to the computer lab and should never leave unattended in the lab or classroom.
- The staff should not install or store new software or programs in computer lab without permission.
- Staff is expected to attend the regular workshops on Internet safety and is responsible to educate the same to students especially about cyber –bullying and possible preventive measures.
- Responsible to educate the students about School Internet policy on regular intervals.

Prohibited Uses of School's Internet by Staff:

- **It is strictly NOT allowed for staff members to use their social media accounts during school hours (as refer to UAE cybercrime law of 2006).**
- It is strictly forbidden for staff to watch any adult website or literature and failure to do so may lead in strict disciplinary action.
- Staff should refrain from download or upload offensive or illegal material.
- Staff should refrain from disseminating any confidential information to unauthorized recipients (Article 378 of the Penal Code (Federal Law 3 of 1987).
- Staff should avoid visiting potentially dangerous websites that can compromise the safety of computers.
- Staff members are prohibited to perform unauthorized or illegal actions such as hacking and online illegal trading.

- Staff members especially teachers are advised to open the content of video or audio before using it in classroom in front of students.
- Staff should not involve themselves in any offensive content to religion.
- Staff members are not encouraged to open their bank details on school devices. As it can motivate to online bank fraudulent.
- Teachers are responsible to always scan their pen drive free form viruses before inserting to any school computer/laptop.
- Using internet to promote their own business motives.
- Indulging in plagiarism and involving in any kind of cyber bullying.
- Teachers are not allowed to use any threatening languages to other member of staff in form of Email communication.
- All staff should protect the downloading and copyrights law of UAE and respect that in any means of downloading the material for personal usage.

Responsibility of Students:

Good Will Children Private School L.L.C. has made the necessary measures to educate students about safe and secure way of using Internet. The school has made the Pledge about internet safety guidelines whereas all students have been made aware of this by ICT teacher which they have to undertake and sign to say that they are responsible for all their actions related internet surfing .

- Students should only visit the websites instructed by theory designated teacher in Computer lab.
- To maintain the maximum security and protecting our devices from harmful viruses, students are not allowed to bring pen drive, hard disk, CD or any other removable devices.
- Students have to comply with all the Computer lab rules while using the computers in Computer lab.
- Students are not allowed to share passwords under any consequences, and violating the same could lead to strict consequences by the school management.
- Students are not allowed to use gaming websites or any other entertainment means while using IL lab.
- Student council members should actively participate in ways to prevent cyber-bullying.
- Students found violating the rules should be immediately reported to the authorities
- Students have to abide with all the protocols mentioned in the online safety policy and agreement form.

Responsibility of Parents:

- The school believes that parents are also equally responsible for educating and monitoring their child's activities about internet at home as the school. The school has encouraged parents to read and understand the student pledge and carry out healthy discussion on safe internet usage with their children.
- To educate the parents about cyber-bullying.
- Parents are responsible to attend the workshop conducted for safe and secure internet usage and should educate the child at home about the same.
- Parents have to ensure that their child/children does not bring any removable devices to school. Any student violating this will face severe consequences from the school management.

Responsibility of Principal:

- The principal of Good Will Children Private School will regularly update the teachers about advancements in Internet safety.
- The principal is responsible to update the policy and will suggest necessary improvements if needed.
- To review the existing Firewall analyzer and update the latest security measures for internet safety measures.
- To monitor and regulate the web usage if staff and students in accordance with IT department on regular basis.
- Circulate a refresher policy to update the important internet security steps that school has taken.

➢ Consequences for violation of this policy:

The School has strict rules and regulation of internet monitoring among students and as a responsible educator the school has set consequences to be followed in order to maintain the internet law and order within the school.

If any student is found violating this policy than appropriate actions will be taken in accordance with our School Behaviour policy. The school management will take positive reinforcement strategies to deal with the violations of this policy and will not punish students academically. The school management has a right to deal with necessary disciplinary measures in case of any violations by the member of the staff.

IN case of any violations of School safe online internet practice, the following protocols will be followed;

- **Level 1:** Initially the students who found violating the rules will be given the verbal warning by the teacher.
- **Level 2:** After two verbal warning, If the student continues to violate the regulations than the teacher has a right to block him for the computer usage in that particular class or period.
- **Level 3:** If the student repeats the behavior in next class, than the teacher needs to contact the social worker who will than called parents to discuss the possible issues.
- **Level 4 :** The written warning is issued to student in case of violation of level 3 and after two written warnings, the school management has right to cancel the extra-curricular activities of that student for period of two weeks .

➢ Monitoring of policy

The Board of Governors, Principal and SLT will regulate the Online Internet Safety policy over regular intervals. In accordance with the School professional standards committees, the members will be encourages to participate actively with proper action plan and further steps of improvement and any areas of concerns will be than identified and proper corrective actions will be taken with support of teachers to further improve the effectiveness of this policy.

Annexure

AGREEMENT FOR BEING SMART ONLINE

Good Will Children Private School understands the importance of technology to develop the student growth and support the same with our parent and students by ensuring the maximum protection and safe usage guidelines.

Parent Consent

I have read and understood the e-safety agreement and give permission for my child to access the Internet at home, and will encourage them to abide by these rules will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Student's Agreement

I have read and I understand the student's e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe.

I _____ agree to the following

- I will be respectful to myself and others. I won't bully and won't tolerate bullying by others.
- I will be a good online friend and be supportive of my friends and others who might be in trouble or in need of help.
- I won't post or send pictures or other content that will embarrass me, get me into trouble or jeopardize my privacy or security.
- I will respect other people's privacy and be courteous when posting photos or other content about them. I'll be conscious of how much time I spend on the web, phone and other devices and won't let use interfere with sleep, school work and face-to-face relationships.
- If they need my help, I'll assist my parents, teachers' others in their use of technology.
- I will respect other people's digital property and space. I won't steal, hack, break into anyone else's accounts or use other's content without permission.
- I will protect my passwords and practice good Net security.
- I will be thoughtful in my use of copy and paste. If I use anyone else's content or images, I will quote them, give them credit and link to them if appropriate.
- I will monitor all the activities on my Microsoft TEAMS and Zoom account and will report any suspicious activities to social worker.
- I will only use my devices for educational purposes as and when requested.
- I will never leave my personal device unattended
- I understand that my personal device is my responsibility and school is not responsible for any breakages, lost or theft or any damage caused by malware of the network.
- I will help create a culture of respect and tolerance during online and among my peers.

Parent Signature: **Student Signature:**

_____ _____

Date: _____ Date: _____