مدرسة وودلم بارك الخاصة

Woodlem Park School Private

E-SAFETY POLICY

2024-2025

Approved By	Principal
Date of Review	March 2024
Next Review Date	March 2025

INTRODUCTION

The impact of technology on the lives of all citizens increases yearly, particularly for children and young people who are keen to explore new and developing technologies. Technology is transforming the way that schools teach, and children learn at home. Technologies are changing the way children live and the activities in which they choose to partake. Developing technology brings opportunities but, the same time it brings risks and dangers too. We, The Woodlem Park School (WPS) is committed to provide a safe and secure learning environment for all our students. The safety and welfare of our whole school community is of the utmost importance.

Ensuring that students can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded program of education. This policy sets out how we will keep students and staff at WPS safe, whether using new technology within WPS provision or at home.

E-safety represents a crucial strand of safeguarding children and vulnerable adults, and such this policy crossreferences to WPS's school policies like Child Protection and Safeguarding Policy and Procedures. This policy applies to all members of the WPS community including staff, pupils/students, volunteers, parents and Guardians, visitors, outside professionals and community users who have access to WPS's ICT system.

This school E-Safety policy describes the policies and practices of The Woodlem Park School, Ajman, related to the online safety and security of the whole school community. Including the procedures, the school must take to ensure the safety and security of the beneficiaries. The E-safety policy of Woodlem Park School demonstrates safe and secure digital practices for the whole school community.

FOREWORD

Nothing is more important that the safety of children. The Woodlem Park School created the E-safety policies to support the whole school community in both protecting children online and providing children with the skills and understanding to protect themselves online.

We, the beneficiaries of The Woodlem Park School are responsible for reading the manual, familiarizing with its contents, and adhering to all the policies, procedures, and protocols of the Woodlem Park School, to ensure the online safety and security of the whole school community.

DEFINITIONS

Safety	E-safety and responsible use of technology. This includes the use of the internet and the other means of communication using electronic devices/media.
Staff	Those who are working for on behalf of The Woodlem Park School Ajman, full time or Part time. And, who have direct or indirect impact on the student's safety and security.
Students	Each learner enrolled at Woodlem Park School, Ajman, including those people of determination and those of special needs.

Parents/ Guardian	The person legally responsible for the student, who enjoys the custody right over him/her or the person entrusted with taking care of him/her.
Visitors	People who visit school for a reason for required and essential service in collaboration.
The whole School community	Refers to all staff, Students, Parents/Guardian and Visitors.
Online Safety Group	A multi -disciplinary team which is concerned to deal with the students' online safety issues, in safety and security terms, and taking the proper decision in this regard, in accordance with the provisions hereof.
Electronic devices	Shall mean any audio or video devices, such as various types of mobile phones, communication and connectivity devices with internet, cameras...etc.
Communication channels	Shall mean any method of communication between the school system, staff, students and the parents/guardians. These channels may include telephone communications, email, SMS, social media and smart notices.
Internet	Refers to the Network technology which is used by the people for information and communication
Social Media	Refers to websites/computer programs used by people to communicate or shareinformation on the internet using electronic devices
Cyber Crimes	Shall mean any unlawfully committed act, including the unauthorized access aiming at threatening or blackmailing a person, compromising his/her private life or causing defamation or harm to him/her, or having access to a private data and disposing thereof, as well as producing what may have an adverse effect on the public order or the religious values.
External agencies	Refers to any government or private agency including, but not limited to, health care, social service, regulatory agencies and police forces.

OBJECTIVES

- To Provide a safe and secure Education and learning environment for the whole school community
- To work to prevent and protect the whole school community from online safety issues through education and Training programs.
- To help to keep children and young people safe online, whether they are using The Woodlem Park School's network and devices.
- To provide clear expectation to the whole school community about the acceptable and unacceptable use of technology.
- To create awareness among the whole school community about the procedure to deal with online safety threats/issues.

ROLES AND RESPONSIBILITIES

A. Principal

- Provide safe and secure Educational Environment to the whole school community.
- Establishing an effective system to address online issues extending such system to the whole school community.

- Support the whole school community with necessary education and training programs related to online safety and security.
- Ensure that the Online Safety Leader and other relevant staff receive appropriate training to enable them to carry out their E-safety roles. That is relevant and regularly updated;
- Review the programs and activities developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.
- Monitoring the effectiveness of the School online Safety Group in managing online safety issues.

B. SLT

- Ensure that the school is having a clear and robust safeguarding procedure are in place for respon ding to online safety issues. And it is well communicated with the whole school community
- Supervising the activities of the Online Safety Leader and other relevant staff.
- Assessing the training needs of the whole school community periodically. And, developed plans to meet the requirements.
- Supervising the reviewing and updating of the school information systems' security regularly.

C. Online safety Group

- To ensure that the E-safety issues are addressed in order to establish a safe digital learning environment.
- To involve in review of school e safety policies and procedures to make; up-to-date amendments to take account of any emerging issues and technologies.
- To provide trainings for staff and thereby update staff about new and emerging technologies so that' the correct E-safety information can be taught or adhered to.
- To deal with the online safety and security related issues in accordance to the procedures as mentioned in the school/nation policies.

D. Online Safety Leader

- The designated Online Safety Leader Shall implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring E-safety is addressed in order to establish a safe digital learning environment.
- Promote the importance of E-safety within school as part of its duty of care to ensure the safety of their pupils and staff
- Ensure that the Acceptable Use Agreements are reviewed annually, with up-to-date information, and that training is available for staff to teach E-safety and for parents to feel informed and know where to go for advice.
- Work alongside the Network Manager to ensure that filtering is set to the correct level for staff, children and young people.
- Equip (i.e. training) children to stay safe online, both in school and outside of school.
- In line with the Prevent/radicalization strategy: Ensure teaching staff are aware of the risks posed by online activities
- Update staff about new and emerging technologies so that the correct E-safety information can be taught or adhered to.
- Work alongside the Network Manager to ensure there is appropriate and up-to-date anti-virus soft ware and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.

To proceed with disciplinary Actions against online safety issues and involve external agencies (law/police) when necessitates

D. IT Supporter

- Provide technical support to ensure the E-safety and security of the whole school community.
- Meet the training necessities of staff and students on E-safety thereby keep them up to date to ensure their online safety and security.
- To advise on the correct use and implementation of filtering categories to ensure age-related filtering is appropriate to education.

E. Social Worker

- Educate children to stay safe online, both in school and outside of school.
- To proceed with disciplinary Actions against online safety issues.
- Provide training for staff and students on procedures to follow on how to deal with online safety issues
- Liaise with the staff to ensure the online safety issues are reporting.
- Monitoring students' online behavior.
- Documenting safety incidents through incidents logbook.

F. Teaching Staff & Support Staff

- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the E-safety Leader.
- Alert the E-safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up to date with E-safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Report accidental access to inappropriate materials to the E-safety officer in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/education setting or other establishment's network.
- Ensure that all personal storage devices (i.e. memory sticks) used by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed "bullying" or other inappropriate behavior via the Internet or other technologies to the safety officer.

G. Parents

- Ensure children's safety and security by monitoring their behavior when they are online.
- Teach children about the acceptable and appropriate online behavior and how to be safe when they are online.
- Report incidents of safety issues or other inappropriate behavior of children to the safety officer.
- To involve in review of school e safety policies and procedures to make; up-to-date amendments to take account of any emerging issues and technologies.

H. Students

- Follow school policies, procedures, and rules to safeguard themselves from online safety threats.
- Use technologies in an appropriate and acceptable manner.
- To involve in the activities related to School E-safety Program through Peer education and support.
- Report incidents of safety-related issues to the safety officer without any delay.
- To involve in the review of school E-safety policies and procedures to make; up-to-date amendments to take

POLICY STATEMENTS

1. Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will adhere to recommended technical standards to ensure optimal performance.
- Safety and security of school technical systems will undergo regular reviews and audits.
- Physical access to servers, wireless systems, and cabling will be restricted to authorized personnel only.
- Access rights to school technical systems and devices will be clearly defined for all users.
- The IT Head will maintain accurate software license logs and conduct regular checks to reconcile purchased licenses with software installations.
- Internet access will be filtered for all users.
- User activity on school technical systems will be regularly monitored and recorded, as outlined in the Acceptable Use Agreement.
- A system will be in place for users to report any actual or potential technical incidents or security breaches to the appropriate person.
- Comprehensive security measures will safeguard servers, firewalls, routers, workstations, and mobile devices against accidental or malicious threats, with regular testing.
- Personal data cannot be transmitted over the internet or taken off-site without encryption or other secure measures.
- Guests/visitors will be required to log in using a visitor login with limited network access.

2. Ensuring Professional Integrity on Social Media

Every school has a responsibility to maintain a safe environment for both students and staff. This includes protecting against potential liabilities arising from the actions of employees, such as harassment, cyberbullying, discrimination, or defamation. To mitigate these risks, the school implements various measures:

Comprehensive Training: Staff members receive training on acceptable social media use, understanding risks, checking privacy settings, data protection, and reporting procedures.

Clear Reporting Guidelines: The school provides clear guidance on reporting incidents, including responsibilities, procedures, and potential sanctions.

Risk Assessment: The school conducts regular risk assessments, including legal risks associated with social media use.

Staff members are expected to adhere to the following guidelines:

Avoid References to School Community: Staff should refrain from mentioning students, parents/caregivers, or colleagues on social media.

Personal Opinions: Personal opinions should not be presented as representing the school or the regulatory authority.

Regular Security Checks: Staff are required to regularly check the security settings on their personal social media profiles to minimize the risk of personal information exposure.

The school's use of social media for professional purposes is monitored regularly by the IT and Social media / Marketing team of the school and e-safety committee to ensure compliance with relevant policies, including those related to social media, data protection, communications, and digital image and video usage.

3. Use of Digital and Video Images

- Staff should inform and educate students about the risks associated with taking, using, sharing, publishing, and distributing digital images. They should particularly emphasize the risks of publishing personal images on the internet, such as on social networking sites.
- Parents/caregivers are permitted to take videos and digital images of their children at school events for personal use. However, to respect privacy and protection, these images should not be publicly shared on social networking sites, and comments involving other students/pupils in the images should be avoided.
- Staff and volunteers may take digital/video images to support educational aims but must adhere to school policies regarding sharing, distribution, and publication. Only school equipment should be used for this purpose; personal equipment of staff is not allowed.
- Care should be taken to ensure that students are appropriately dressed and not engaging in activities that could bring individuals or the school into disrepute when taking digital/video images.
- Students must not take, use, share, publish, or distribute images of others without their permission.
- Photographs including students published on the website or elsewhere will be selected carefully and will comply with good practice guidance.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Social media Consent from parents or carers will be obtained before photographs of students are published on the school website.

4. Acceptable Use

Pupil/student rules for acceptable internet use

We will adopt the rules as laid out below in an age-appropriate way for the pupils/students at Woodlem Park School.

- I will ask permission from an adult before using the Internet.
- I will use computers and tablets safely.
- I will not look for websites that I know I'm not allowed to see.
- If I see anything that I know is wrong I will tell an adult straight away.

Visitor rules for acceptable internet use

Visitors' Internet use will vary depending upon the purpose of their visit. Generally, we expect all visitors to abide by the following rules:

- I will respect the facilities by using them safely and appropriately.
- I will not use the Internet for personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant or upsetting material to a member of staff immediately.
- I will not download or install program files.
- I will not use USB memory devices on computers.

- I will be polite and respect others when communicating over the Internet.
- I will not share my login details.
- I will not carry out personal or unnecessary printing.
- I understand that they may check my computer files and monitor my Internet use.

⬘ Staff rules for acceptable internet use

Staff must use the Internet safely, appropriately and professionally within the. They must be aware that they are role models for others and should promote and model high standards of behavior at all times. For further details please refer to the Woodlem Park School IT Acceptable Use Policy.

5. Education and Training

The aim of E-safety education within Woodlem Park School is to teach pupils and students how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

Pupils/students will be taught about safe and appropriate electronic communication, including the indelible nature of emails, social media presence, images and other E-communications. Aspects of E-safety such as cyberbullying, revenge porn, trolling and other harassment will be covered in an age-appropriate way, with emphasis placed on respecting oneself and one's peers, in order to build confidence and understanding among pupils/students as they interact with technology.

For younger pupils/students Internet use will be closely supervised and based around pre-selected, safe websites. Pupils/students will be regularly reminded about how to always take care when clicking and to seek help from an adult if they see anything that makes them unhappy or that they are unsure about. These digital literacy skills will be developed in keeping with pupils'/students' age and ability, with lessons promoting a responsible attitude towards searching the Internet and the importance of personal security measures such as strong passwords and processes for reporting any concerns.

As they progress through the, pupils/students will be encouraged to become more independent at researching information on the Internet, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported to use online collaboration tools for communicating and sharing ideas.

⬘ E-safety updates for staff

Staff will receive regular updates about how to protect and conduct themselves professionally online and to ensure that they have an awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues. Some of this information will be provided by email updates and at staff meetings.

⬘ E-safety updates for parents/care givers

WPS aims to provide opportunities for parents and care givers to receive E-safety education and information (e.g. via the website) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good E-safety.

⬘ Guidance on the use of social networking and messaging systems

Woodlem Park School recognizes that many staff will actively use Facebook, Twitter and other social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognize that it is not appropriate to discuss issues relating to pupils/students or colleagues via social media networks; discretion and professional conduct is essential. Posts that bring Woodlem Park School into disrepute and/or breach confidentiality are likely to result in disciplinary action. Staff should review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

It is never acceptable to accept a friendship request from a child or young person in an Woodlem Park School provision or from ex-pupils/students who are still minors. This is to avoid any possible misinterpretation of motive or behavior which could be construed as grooming.

Staff must not give their personal contact details to pupils/students, including E-mail, home or mobile telephone numbers. All correspondence should be via Woodlem Park School systems.

6. Data Protection

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimizing the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' or 'locked' at the end of any session in which they are using personal data;
- Be fully aware of the risks of transferring data using removable media. When personal data is stored on any portable computer system, USB stick or any other removable media, it must be securely deleted once its use is complete.

It may sometimes be necessary to send confidential information outside the organization e.g. as part of a safeguarding investigation. Woodlem Park School staff must at all times consider the security of such information. Any confidential or sensitive information conveyed via email must be password protected and the password conveyed separately to the recipient, preferably by means other than email. Confidential or sensitive emails should be encrypted wherever possible.

7. Bring Your Own Device (BYOD)

Rules for Bring your Own Device (BYOD)

1. Device Compatibility:
Ensure that devices brought to school are compatible with the school's network and technology requirements.

2. Responsible Use:
Users must adhere to school policies regarding acceptable use of technology, including appropriate online behaviour, respect for others' privacy and refraining from accessing inappropriate content.

3. Security Measures:
Devices should have up-to-date antivirus software and security setting enable to protect against malware and unauthorized access

4. Network Access:
Users must connect only to authorized school networks and refrain from creating personal hotspots or sharing netwok access without permission.

5. Data Protection:
Users are responsible for safeguarding their own data and ensuring that sensitive information is not shared or stored inappropriately.

6. Respect for Learing Environment:
Devices should be used for educational purposes only during designated times and in approved areas to minimize distractions and disruptions to the learning environment.

7. Compliance with School Policies:
BYOD users must comply with all school policies related to technology, including those regarding copyright, intellectual property rights and software licensing.

8. **Reporing Misuse:**
Any misuse or unauthorized access involving BYOD devices should be promptly reported to school administration or IT staff for investigation and appropriate action.

9. **Liability:**
Users are solely responsible for the care and maintenance of their devices, and the school is not liable for any damage, loss or theft of personal devices onto school premises.

10. **Agreement:**
Prior to bringing a device to school, users and parents/ guardians must sign an agreement acknowledgeing their understanding and acceptance of the BYOD rules and guidelines.

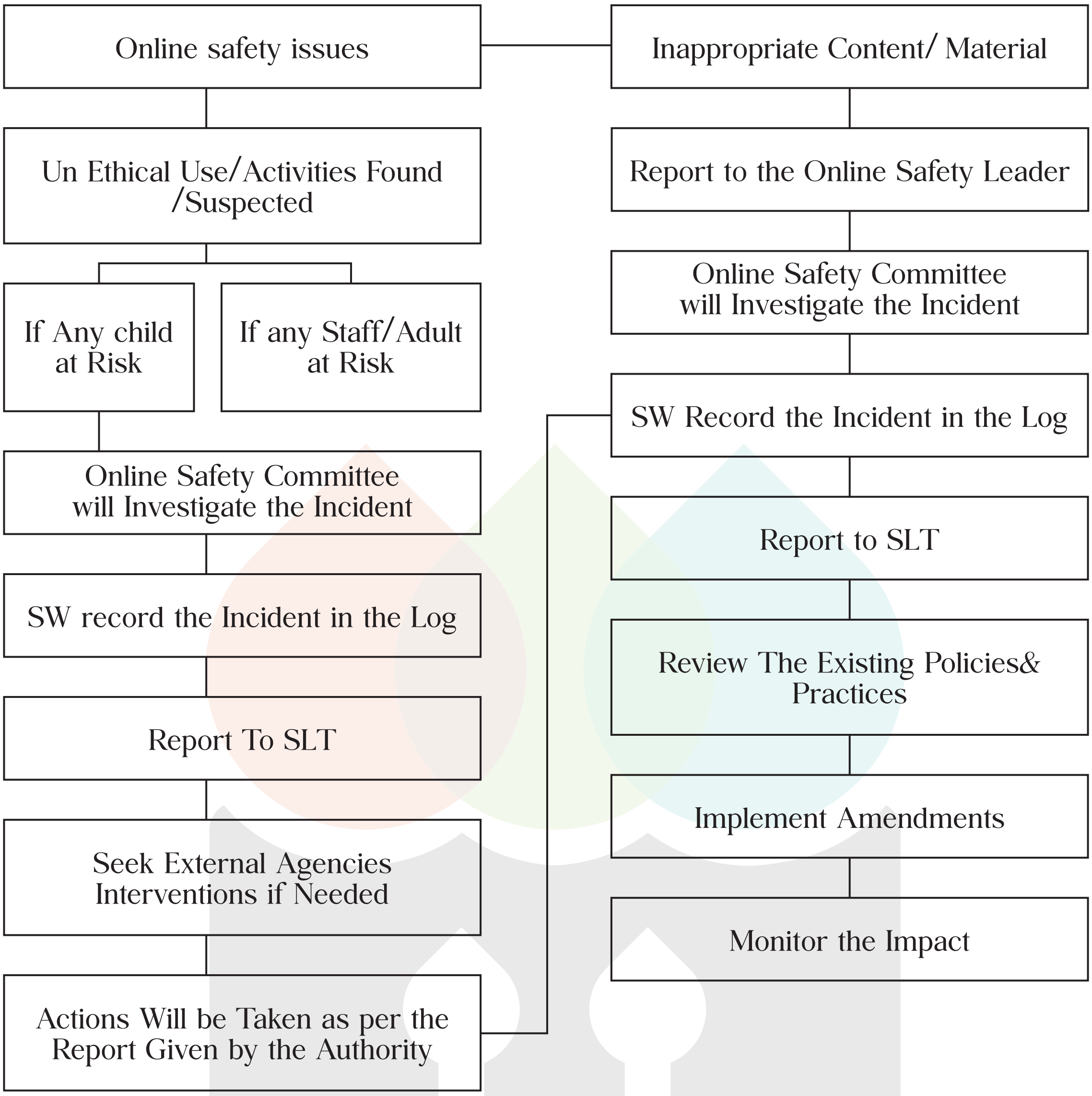
8. Responding to incidents:

It is more probable that the school will need to handle incidents involving inappropriate rather than illegal misuse. It is crucial to address any incidents promptly and proportionately, ensuring that members of the school community are informed about the resolution.

The online safety committee will address incidents, discuss them, and escalate them with the assistance of the Online Safety Leader and school social workers.

ONLINE SAFETY COMMITTEE	
Principal	Ms. Pranati Mazumder
SLT	Vice Principal Head of Teaching and Learning Head of Section (9 to 12) Head of Section (5 to 8) Head of Section (1 to 4) Head of Section (KG)
Admin Manager	Mr. Shafeeque KC
Online Safety Leader	Incharge- Department of Computer Science
Staff Representatives	Head of IT Head of Inclusion School Counsellors Computer Science Faculty Member
Student Representatives	Student Council Members
Parent Representatives	PTC Member

ESCALATION PROCEDURE


Online safety issues
Un Ethical Use/Activities Found /Suspected
If Any child at Risk
If any Staff/Adult at Risk
Online Safety Committee will Investigate the Incident
SW record the Incident in the Log
Report To SLT
Seek External Agencies Interventions if Needed
Actions Will be Taken as per the Report Given by the Authority
Inappropriate Content/ Material
Report to the Online Safety Leader
Online Safety Committee will Investigate the Incident
SW Record the Incident in the Log
Report to SLT
Review The Existing Policies& Practices
Implement Amendments
Monitor the Impact

CROSS REFERENCE

- The child Protection & Safeguarding Policy of WPS
- School Health& Safety Policy
- Acceptable Use Policy
- Social Media Policy
- Mobile device/BYOD Policy
- Data Protection Policy
- Password Policy
- Filtering Policy
- The student behavior management policy no: 851 of year 2018
- Students' behavior Management Policy 2018
- UAE's Federal Law 5 of 2012
- UAE's Federal Law 12 of 2016
- UAE's Federal Law 34 of 2021